Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Op Weg naar Weerbare Virtualisatie

Keuzes voor continuïteit, digitale autonomie en verminderen leveranciersafhankelijkheid

13 april 2026

Versie 1

accenture

Inhoud

Managementsamenvatting

Overheidsorganisaties staan voor een strategisch vraagstuk rond hun digitale infrastructuur. De combinatie van veranderende licentiemodellen (1.2.1, Appendix B), sterke leveranciersafhankelijkheid en geopolitieke onzekerheden (1.2.2) legt structurele kwetsbaarheden bloot in de huidige inrichting van virtualisatie- en platformvoorzieningen. De overname van VMware door Broadcom (1.2.1) en de overgang naar een verplicht abonnementsmodel laten hierbij zien dat zonder bewuste keuzes het risico groot is op meer afhankelijkheid van één leverancier, tegen hogere kosten en met minder onderhandelingsruimte. Dit raakt de verantwoordelijkheid van overheidsorganisaties voor continuïteit van dienstverlening en beheersbaarheid van kosten, en roept binnen organisaties verschillende vragen op:

- Hoe krijgen we inzicht in de afhankelijkheid op VMware?
- Hoe verminderen we de afhankelijkheid op leveranciers van software?
- Hoe kunnen we het IT-landschap bestendiger maken tegen risico's die de continuïteit van dienstverlening bedreigen?
- Welke aspecten moeten we rekening mee houden bij het herijken van de strategie?
- Hoe ziet een selectieproces voor een nieuw platform eruit en welke criteria moeten we daarbij toepassen?
- Welke aspecten moeten we rekening mee houden als we migreren naar een nieuw platform?

Dit rapport biedt handvatten om deze vragen te beantwoorden. Het rapport is niet voorschrijvend bedoeld, maar faciliterend om handelingsperspectief te bieden aan overheden. Het maakt duidelijk dat de keuze voor een virtualisatieplatform geen louter technische of tactische beslissing is (hoofdstuk 2), maar een strategische keuze met langdurige gevolgen voor governance, organisatie, leveranciersmanagement en risicobeheersing. Binnen de context van rijksbreed beleid, de Nationale Digitaliseringsstrategie en toenemende politieke aandacht voor digitale autonomie, is het noodzakelijk dat overheidsorganisaties expliciet bepalen waar zij afhankelijkheden accepteren en waar zij deze actief willen beperken (1.2.2). Niet alle afhankelijkheid is vermijdbaar of ongewenst, maar onbewuste of onbeheerste afhankelijkheid vormt een reëel risico voor de continuïteit van publieke dienstverlening.

Een belangrijk inzicht is dat niet alle systemen en applicaties gelijk zijn (2.1). Overheidslandschappen bestaan uit een mix van hoog kritische systemen, gevoelige gegevensverwerkingen en minder kritische ondersteunende toepassingen. Door applicaties te categoriseren op basis van deze eigenschappen ontstaat ruimte voor gedifferentieerde keuzes in architectuur en platformstrategie (2.1, 2.2). Zwaardere eisen aan autonomie, exit-mogelijkheden en continuïteit kunnen gericht worden toegepast waar de maatschappelijke impact van uitval of afhankelijkheid het grootst is, terwijl voor minder kritische systemen kostenefficiëntie zwaarder kan wegen. Dit voorkomt zowel over-engineering als ongewenste risico's.

Het rapport laat zien dat er meerdere strategische richtingen mogelijk zijn (2.2):

- Optimalisatie van de bestaande omgeving;
- Migratie naar een alternatief platform;
- Parallel inzetten van meerdere platformen;
- Kiezen voor open standaarden
- (Gedeeltelijke) inzet van open source oplossingen.

Geen van deze opties is zonder consequenties. Alternatieven voor de huidige dominante platforms vragen vrijwel altijd om investeringen in nieuwe kennis, aanpassingen in beheerprocessen en een herziening van de samenwerking tussen platformteams en applicatieteams. Met name keuzes richting open standaarden, containerplatformen of open source vergroten op termijn de wendbaarheid, maar vragen op korte termijn meer regie,

volwassen governance en expliciete investeringen in expertise (2.1). Dit betekent dat platformkeuzes niet los gezien kunnen worden van organisatie-inrichting en verandermanagement. De transitie naar een toekomstbestendige platformstrategie raakt rollen, verantwoordelijkheden en competenties binnen de IT-organisatie, en vraagt om nauwe betrokkenheid van finance, inkoop en HR (2.3). Ook leveranciersmanagement verandert van een primair operationele activiteit naar een strategisch instrument, waarin exit-strategieën (2.2.1), licentiemodellen en overname-clausules (2.3.2.2) standaard onderdeel moeten zijn van besluitvorming en contractering. Een additionele mitigerende maatregel kan ook applicatie modernisatie zijn om zo onafhankelijkheid te creëren van de onderliggende infrastructuur (2.3.3.2).

Een cruciaal bestuurlijk aandachtspunt is tijdigheid (2.3). De selectie en implementatie van een nieuw virtualisatie- of platformlandschap vergt in de praktijk één tot meerdere jaren, zeker in complexe omgevingen. Uitstel vergroot het risico dat organisaties onder tijdsdruk gedwongen worden tot suboptimale keuzes, bijvoorbeeld bij het aflopen van contracten of onverwachte prijswijzigingen. Vroegtijdige besluitvorming biedt ruimte voor een gecontroleerde, gefaseerde aanpak waarin risico's beheersbaar blijven en continuïteit is geborgd. Deze gefaseerde aanpak (2.3) en de besliscriteria (hoofdstuk 3) om verschillende oplossingen tegen elkaar af te zetten worden in dit rapport beschreven, en de besliscriteria zijn ook toegepast op de virtualisatieplatforms die binnen de overheid gebruikt worden of als kansrijk alternatief worden gezien (Appendix C).

Samenvattend (Hoofstuk 4) onderstreept het rapport dat overheidsorganisaties expliciete strategische keuzes moeten maken over hun platformstrategie. Door virtualisatie en platformen te benaderen als een bestuurlijk dossier – waarin kosten, risico's, autonomie en organisatieontwikkeling integraal worden afgewogen – kunnen overheidsorganisaties regie houden over hun digitale infrastructuur. Dit stelt hen in staat om publieke dienstverlening duurzaam te ondersteunen, beter voorbereid te zijn op geopolitieke en marktontwikkelingen en de digitale weerbaarheid van de overheid als geheel te versterken.

Zie in onderstaande overzichten de belangrijkste conclusies en aanbevelingen uit hoofdstuk 4. De aanbevelingen kennen een volgordelijkheid op basis van prioriteit en verankering in de organisatie (4.4).

Conclusies

1. Virtualisatie is niet meer alleen **een IT-only onderwerp**, maar een **strategisch bestuursdossier** met impact op continuïteit, kosten, governance en leveranciersrisico's.

2. **Autonomie en weerbaarheid gaan verder dan infrastructuur**; het applicatielandschap, architectuur, operatie en interne expertise zijn doorslaggevend.

3. Het **één-op-één vervangen** van virtualisatietechnologie **verplaatst afhankelijkheid**, maar lost deze niet structureel op.

4. Leveranciersonafhankelijkheid kent **meerdere routes** (exit, multi-vendor, open standaarden), elk met **organisatorische en governance-impact**.

5. Open source kan afhankelijkheid **verminderen**, maar **neemt deze niet volledig weg** en vraagt een ander operationeel model.

6. Er **is niet één oplossing** die voor alle organisaties van toepassing is.

Aanbevelingen

Stuur programmatisch op het applicatielandschap:

- Voer structurele **applicatie-portfolio-optimalisatie en -rationalisatie uit.**
- Categoriseer applicaties op **(geo)politieke risico's, continuïteits- en impactniveau.**
- Koppel categorieën aan passende **architectuur-archetypes**.

Maak exit en verplaatsbaarheid standaard:

- Veranker een **exitstrategie** in selectie, contractering en lifecycle-management.
- Eis van leveranciers **exit zonder boetes** en **technische ondersteuning bij overstap**.

Hanteer duidelijke technologie- en leverancierprincipes:

- Gebruik **open en de-facto standaarden** waar mogelijk.
- Overweeg **meerdere leveranciers** waar segmentatie mogelijk is en de organisatorische overhead beheersbaar blijft.
- Pas proprietary technologie alleen toe als **verplaatsbaarheid aantoonbaar** is.

Versterk governance en integraliteit:

- Herevalueer risicos frequent om zo in controle te blijven en te kunnen anticiperen op externe factoren.
- Start trajecten **tijdig** en betrek **Finance en HR** expliciet vanwege kosten-, skills- en organisatie-impact.

Hoofdstuk 1 - Context

1.1 Inleiding

De digitale infrastructuur van overheidsorganisaties staat onder druk door ingrijpende veranderingen in de markt en het internationale speelveld. De recente overname van VMware door Broadcom en de bijbehorende wijziging van het licentiemodel hebben grote gevolgen voor de gebruikskosten van VMware en leggen bloot dat er sprake is van een significante leveranciersafhankelijkheid (vendor lock-in). Leveranciersafhankelijkheid – van VMware in het bijzonder en andere leveranciers in het algemeen – heeft naast kostenstijgingen invloed op de strategische autonomie en weerbaarheid van organisaties die afhankelijk zijn van specifieke software. In het kader van de geopolitieke ontwikkelingen en het groeiende belang van digitale soevereiniteit dient deze afhankelijkheid meegenomen en geëvalueerd te worden in de herijking van het IT-beleid van de overheid.

Dit rapport biedt inzicht in de keuzes die gemaakt moeten worden bij het (her)overwegen en vervolgens eventueel selecteren en implementeren van applicaties en het (virtualisatie) platform waarop deze draaien, met bijzondere aandacht voor de impact van licentiemodellen, afhankelijkheden van leveranciers en de bredere strategische doelstellingen van de organisatie. Het document reikt handvatten aan voor het uitvoeren van risicoanalyses, het bepalen van migratiestrategieën en het opstellen van besliscriteria, zodat organisaties weloverwogen en toekomstbestendige keuzes kunnen maken voor hun IT-landschap.

1.2 Aanleiding

De directe aanleiding voor dit rapport is de ingrijpende wijziging in de licentiestructuur van VMware na de overname door Broadcom in november 2023. Naast dat die overname specifieke vragen rondom VMware naar voren brengt, heeft dit ook geleid tot bredere zorgen rondom afhankelijkheid (lock-in) van leveranciers. Veranderingen in de geopolitieke situatie zorgen daarnaast voor bredere zorgen rondom de digitale autonomie en weerbaarheid van de overheid, hetgeen invloed heeft op het bredere IT-beleid.

1.2.1 VMware overname door Broadcom en leveranciersafhankelijkheid

De wijzigingen die Broadcom heeft doorgevoerd in de licentiestructuur van VMware betreft niet alleen een aanpassing van prijzen, maar een complete transformatie van het product- en dienstenaanbod en het licentiemodel, met verstrekkende gevolgen voor organisaties. Per 1 januari 2024 heeft Broadcom het traditionele licentiemodel voor VMware op basis van “perpetual” licenties vervangen door een abonnementsmodel (zie Appendix B – Licentievormen voor detailinformatie). In het oude model kreeg een organisatie een eeuwigdurend gebruiksrecht, waarnaast contracten afgesloten konden worden voor onderhoud (updates, patches en bugfixes) en (technische) ondersteuning.

In het nieuwe abonnementsmodel is er geen eeuwigdurend recht meer. Een organisatie mag de software gebruiken en krijgt onderhoud en ondersteuning zolang voor het abonnement betaald wordt. Zonder actief abonnement verliest de organisatie toegang tot de software en het recht om het te mogen gebruiken, wat resulteert in verlies van functionaliteit. Verder hadden organisaties in het oude model meer keuze in het afnemen van licenties voor die producten die ze nodig hadden, terwijl in het nieuwe model meer producten gebundeld zijn waardoor de flexibiliteit vermindert. Deze wijzigingen hebben o.a. de volgende gevolgen:

- Budgettaire druk door fors hogere kosten en periodieke prijsstijging (10% per jaar).
- Geforceerde upgrades naar de meest recente versie.
- Mogelijke verdere vendor lock-in door kosten efficiënt met bundels om te gaan.
- Verlies van functionaliteit bij eindigen abonnement.

Bij elkaar legt dit bloot dat (IT-)organisaties afhankelijkheden (kunnen) hebben op leveranciers van IT-systemen en dat deze afhankelijkheid organisaties zowel financieel als operationeel kwetsbaar maken. Daarmee lopen kritieke processen binnen de Nederlandse overheid risico wanneer software niet deugdelijke functioneert of niet meer beschikbaar is.

Omdat bij abonnementen de functionaliteit niet meer beschikbaar is zodra niet meer betaald wordt voor het abonnement, raakt dit de kern van de strategische autonomie van rijksorganisaties. Organisaties verliezen de mogelijkheid om tijdelijk niet te verlengen, om druk uit te oefenen in onderhandelingen, of om gefaseerd over te stappen. Waar het besluit om te verlengen bij perpetual licenties een strategische keuze was, is het bij abonnementen een operationele noodzaak geworden. Dit vereist een andere manier van werken.

1.2.2 Verandering van de geopolitieke situatie

De huidige geopolitieke situatie zorgt voor urgentie om strategische afhankelijkheden te verkleinen. De afhankelijkheid van niet-Europese technologiebedrijven, met name Amerikaanse aanbieders, is door recente internationale spanningen en incidenten een belangrijk thema geworden. Op zowel nationaal als Europees niveau groeit het besef dat digitale autonomie en soevereiniteit essentieel zijn voor de continuïteit van publieke dienstverlening en de bescherming van publieke waarden.

Dit wordt onderstreept door het kabinetsbeleid vanuit de Nationale Digitaliseringsstrategie (NDS)[1], waarin digitale weerbaarheid en digitale autonomie een van de zes prioriteiten is, en de Digitale Open Strategische Autonomie (DOSA)[2], waarin de afhankelijkheden op geïmporteerde technologie als risico aangemerkt worden. De visie 'Digitale autonomie en soevereiniteit van de overheid' is in deze ook goed om te benoemen. Centraal in deze visie staan "het verminderen van ongewenste strategische afhankelijkheden, het vergroten van technologische zelfredzaamheid en het stimuleren van samenwerking binnen Europa."[3] Ook vanuit de Tweede Kamer is voor dit onderwerp veel aandacht en wordt middels verschillende instrumenten invloed uitgeoefend op het kabinetsbeleid (details in Appendix A – Moties en kamervragen):

- Moties tijdens het debat omtrent afhankelijkheid Amerikaanse techbedrijven;
- Kamervragen over de groeiende afhankelijkheid van Amerikaanse techgiganten;
- Initiatiefnota Wolken aan de horizon[4];
- Kamervragen over de overnames van Zivver en Solvinity;
- Kamervragen over de overstap Belastingdienst naar Microsoft;
- Kamervragen over de afhankelijkheid van de financiële sector van Amerikaanse techgiganten.

Hoewel dit meer gericht is op het gebruik van Cloud en de risico's dat buitenlandse mogendheden toegang krijgen tot overheidsdata via gerechtelijk bevel, speelt hier ook het risico dat diensten niet meer geleverd kunnen worden of software niet meer bijgewerkt wordt door doordat de overheid van het land waarin de leverancier gevestigd is dit blokkeert. Dit is in feite een andere manier waarop vendor lock-in tot problemen kan leiden en waarom data risico meegewogen moet worden bij pakketselectie en de bredere inrichting van het IT-landschap. De motie 26643-1318: Risicoanalyse en Exit-strategie voor clouddiensten van Amerikaanse Techgiganten is daarom eigenlijk breder van toepassing.

Tot slot is er ook een breder strategisch en economisch belang voor Nederland en Europa, zoals uitgedrukt in motie 26643-1323: Europese bedrijven op één te zetten bij aanbestedingen van vitale ICT-diensten en voor de rijksoverheid en lokale overheden samen met het bedrijfsleven alternatieven te ontwikkelen voor de grote Amerikaanse techbedrijven.

1.3 Opdracht en Opdrachtgever

Om de rijksoverheden te faciliteren in het besluitvormingsproces over de toekomstige omgang met VMware software is besloten om een adviesrapport op te laten opstellen. Het adviesrapport is bedoeld voor organisaties vallend onder de kerndepartementen, evenals de diensten, agentschappen en adviescolleges (Uitvoeringsorganisaties) ressorterend onder de kerndepartementen. Zelfstandige bestuursorganen (ZBO's) zijn zelfstandig verantwoordelijk voor ICT-vraagstukken, maar het rapport zal ook met hen worden gedeeld. Tevens zal het rapport, conform de aanpak onder de NDS, ter kennisname gedeeld worden met medeoverheden, zoals VNG, IPO en Waterschappen.

De organisaties die deelnemen aan het initiatief (verder: deelnemers) verschillen in grootte (klein, middel, groot) en in het gebruik van VMware (beperkt, gemiddeld, veel). De deelnemers kennen vele prioriteiten op ICT gebied; denk aan cyber security, invoering AI, personeelstekorten enz. Een aantal deelnemers kan zelfstandig de Vmware problematiek het hoofd bieden, andere deelnemers hebben behoefte aan ondersteuning en advisering. Waar in het algemeen kennis ontbreekt bij de deelnemers is het doel van deze opdracht om hierin tegemoet te komen door middel van een adequaat en gedragen adviesrapport.

De opdrachtgever van dit adviesrapport is de Taskforce Continuïteit ICT Dienstverlening (CID) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[1] Nederlandse Digitaliseringsstrategie (NDS) - Digitale Overheid. https://www.digitaleoverheid.nl/nederlandse-digitaliseringsstrategie-nds/
[2] Agenda digitale open Strategische autonomie. Rapport | https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa
[3] Visie 'Digitale autonomie en soevereiniteit van de overheid | https://www.rijksoverheid.nl/documenten/rapporten/2025/12/18/bijlage-2-visie-digitale-autonomie-en-soevereiniteit-van-de-overheid
[4] Initiatiefnota Wolken aan de horizon. Publicatie | https://www.rijksoverheid.nl/documenten/publicaties/2024/06/18/initiatiefnota-wolken-aan-de-horizon

1.4 Doelstelling

Bij een pakketselectie spelen over het algemeen met name tactische overwegingen een rol, zoals de technologie, gebruiksgemak, ondersteuning van de leverancier, en de totale kosten over de levensduur (total cost of ownership). Zowel de verandering in licentiemodellen als de huidige (geo)politieke situatie vereist echter dat met een bredere blik gekeken wordt naar strategische doelstellingen alvorens over te gaan tot pakketselectie voor onderdelen van de IT-diensten die de organisatie moet ondersteunen.

Hierbij speelt enerzijds een rol dat nieuwe licentiemodellen invloed hebben op hoe keuzes gemaakt kunnen worden. Daarnaast vraagt de (geo)politieke situatie om anders te kijken naar vendor lock-in. Om weloverwogen keuzes te kunnen maken, moeten organisaties hun governance aanpassen en strategische informatie verzamelen over het asset landschap, afhankelijkheden en risico's. Dit rapport behandelt daarom ook de strategische opties voor rijksorganisaties en biedt handvatten voor besluitvorming over de toekomst van hun IT-landschap in het algemeen en de virtualisatie infrastructuur in het bijzonder.

Vanuit het bovenstaande heeft dit rapport drie doelstellingen:

1. Inzicht bieden in de keuzes die gemaakt moeten worden bij het (her)overwegen van de selectie en implementatie van een virtualisatieplatform.
2. Inzicht bieden in hoe overheidsorganisaties minder afhankelijk worden van specifieke leveranciers.
3. Een strategisch inzicht bieden rondom autonomie en weerbaarheid, om geopolitieke afhankelijkheden te verminderen.

Vanuit de directe aanleiding staat de keuze van een virtualisatieplatform bovenaan, hoewel dit het meest tactische onderdeel is. Om deze onderwerpen van strategisch naar tactisch te behandelen, worden deze onderwerpen in omgekeerde volgorde behandeld.

1.5 Leeswijzer

Dit document kent meerdere doelgroepen, te weten CIOs, CTOs en (Enterprise) Architecten en heeft meerdere doelstellingen.

CIO
Het hoofdstuk 2 Handelingsperspectief/Aanpak is onderverdeeld naar de drie verschillende doelstellingen. CIOs zullen met name geïnteresseerd zijn in de meer strategische doelstellingen en daarmee de volgende twee secties:

- 2.1 Strategische aanpak autonomie en weerbaarheid
- 2.2 Verminderen van leveranciersafhankelijkheid

Voor de meer operationele doelstelling ten aanzien van de keuze voor een virtualisatieplatform, zullen CIOs meer interesse hebben in de secties die een overzicht bieden van de aanpak en de besliscriteria, te weten:

- 2.3.1 Oplossingsstrategie
- 2.3.2 Overzicht selectie- en implementatieproces
- 3.1 Overzicht van de besliscriteria

Het verdere overzicht en verdieping wordt besproken in:

- 4 Conclusies en aanbevelingen
- Appendix A – Moties en kamervragen
- Appendix B – Licentievormen

CTO
CTOs zullen door hun meer technische profiel naast het bovenstaande met name geïnteresseerd zijn in de volgende secties:

- 2.3 Selectie en implementatie virtualisatie platform
- Het overzicht van platform in Appendix C – Virtualisatieplatformen

(Enterprise) Architecten
(Enterprise) Architecten zullen meer interesse hebben in de afwegingen, het proces en de besliscriteria, en daarmee in de volgende secties:

- 2.1.3 Oplossingsarchetypen definiëren
- 2.1.4 Organisatiestructuur en processen
- 2.3 Selectie en implementatie virtualisatie platform
- 3 Besliscriteria
- 4 Conclusies en aanbevelingen
- Appendix C – Virtualisatieplatformen
- Appendix D – Andere alternatieven

Hoofdstuk 2 - Handelingsperspectief/Aanpak

2.1 Strategische aanpak autonomie en weerbaarheid

Zoals besproken in de aanleiding en doelstelling is de geopolitieke situatie een van de belangrijkste drijfveren om technisch beleid te herijken. De zorgen spitsen zich grofweg toe op twee zaken:

- Toegang of toe-eigening van data door een buitenlandse mogendheid.
- Het niet meer kunnen uitvoeren van overheidstaken doordat technologie niet meer beschikbaar is.

De huidige denkrichting van de Tweede Kamer en breder in de maatschappij is daarbij dat het beste is om alle infrastructuur in eigen datacentra te plaatsen en de infrastructuur en software geheel zelf te beheren, hetgeen gereflecteerd wordt in motie 26643-1316: *Aanbesteding voor een rijkscloud in volledig Nederlands beheer.*

Dit is een mooi streven, maar voor dat een zogenaamde Rijkscloud gerealiseerd kan worden zijn er nog wel een aantal punten die aandacht verdienen. De vraag is ook of je als overheid direct wil concurreren met grote cloud providers als het gaat om de hoeveelheid diensten en prijs. Een afgeslankte versie met essentiële dienstverlening is daarom ook een betere optie. Hoewel hogere kosten voor het volledig zelf beheren van de infrastructuur vanuit het oogpunt van strategische autonomie acceptabel kunnen zijn, moet ook in acht genomen worden dat hiervoor (specialistische) expertise vereist is die de overheid over het algemeen niet zelf in huis heeft en zelfs de vraag gesteld kan worden of deze in voldoende mate aanwezig is binnen de landsgrenzen. Het gaat hierbij onder andere om een veelzijdigheid aan kennis ten aanzien van het ontwerpen, bouwen, beveiligen en opereren van datacentra, (landelijke) glasvezelnetwerken, CPUs en andere hardware, platform software, en diensten. Zelfs voor de grote Amerikaanse cloud providers geldt dat deze expertise niet alleen uit de eigen gelederen komt en dat experts uit allerlei landen komen. AWS, Google, en Microsoft hebben allen ook ontwikkelteams in onder andere India en meerdere Europese landen, en gebruiken toeleveranciers voor allerlei producten en diensten. Zij hebben daarom ook allerlei processen om supply chain management op grote schaal te doen.

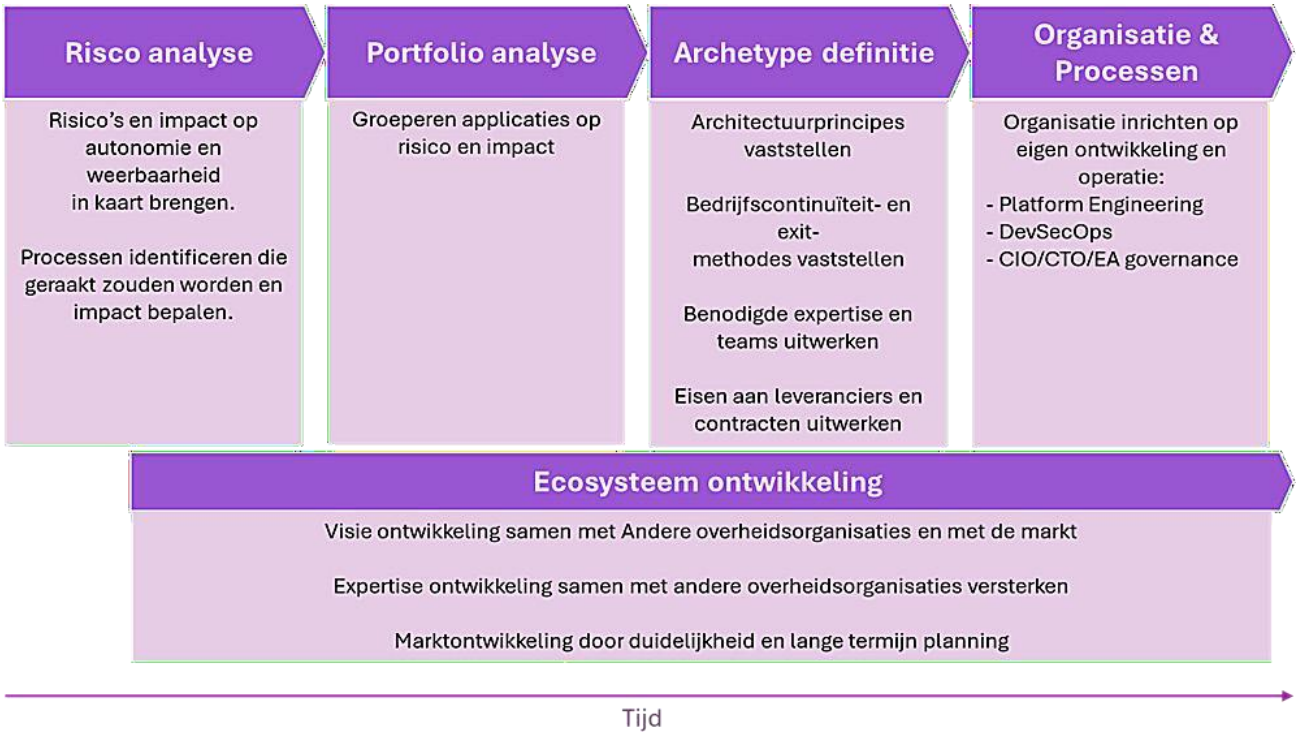
Een ander aspect is de vraag of de huidige organisatie van de overheid en de manier waarop budgetten gealloceerd worden wel aansluit bij een centrale cloud voorziening in eigen beheer. De (budgettaire) autonomie van ministeries en instanties die daaronder vallen, als ook van provincies en gemeenten, maakt het ingewikkeld om krachten en budgetten te bundelen zodat diensten centraal ontwikkeld kunnen worden. Onder de huidige (wettelijke) structuur kan dit met name met vrijwillige samenwerkingsverbanden, waarbinnen afspraken gemaakt moeten worden over welke partijen budget leveren voor bepaalde activiteiten.

De inval van Oekraïne en de aanpak van landen als Estland die onder constante dreiging van inval door Rusland staan, laat zien dat alles onder eigen controle hebben niet per definitie beter is. Oekraïne heeft in recordtempo overheidsservers in de cloud[5] moeten plaatsen en met vrachtwagens moeten verschepen naar datacentra in andere landen.

Estland werkt al meer dan 10 jaar met een concept van data ambassades[6] waar back-ups bewaard worden van essentiële data en diensten, zodat overheidsorganisaties door kunnen gaan wanneer datacentra in eigen land niet meer beschikbaar zijn. Dit laat zien dat wat nodig is voor autonomie en weerbaarheid verschilt per scenario, waarbij het volledig afdekken van alle risico's van alle scenario's enorme kosten met zich meebrengen. Er moeten dus bewuste keuzes gemaakt worden ten aanzien van welke risico's acceptabel zijn voor welke systemen onder welke omstandigheden.

Daarbij moet een evenwicht gevonden worden tussen functionaliteit, veiligheid, flexibiliteit, standaardisatie, autonomie, en kosten. Alleen voor de meest kritische systemen zullen kosten een ondergeschikt belang vormen. Het rapport "Van kwetsbaar naar weerbaar"[7] geeft concrete aanbevelingen ten aanzien van hoe de overheid als organisatie met de geopolitieke afhankelijkheden om moet gaan en welke zaken daarvoor ingeregeld moeten worden binnen de overheid. De onderstaande aanpak (zie pagina 9) gaat dieper in op hoe een organisatie binnen de overheid om kan gaan met deze risico's vanuit een procesmatige aanpak.

[5] Oekraïne zette al 15 petabyte in de AWS-cloud - Computable.nl. Computable.nl. https://www.computable.nl/2024/01/05/oekraine-zette-al-15-petabyte-in-de-aws-cloud/
[6] A world first: Estonia opens a "data embassy" in Luxembourg. https://www.blue-europe.eu/analysis-en/short-analysis/a-world-first-estonia-opens-a-data-embassy-in-luxembourg
7 "Van kwetsbaar naar weerbaar." Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar



Figuur 1: Een procesmatige aanpak van hoe overheidsorganisaties kunnen omgaan met de risico's van geopolitieke afhankelijkheden.

2.1.1 Risicoanalyse

Om de juiste strategische overwegingen te maken, dienen de risico's en de impact daarvan in kaart gebracht worden. Dit is een proces wat al gebeurt binnen de overheid, maar aangezien dit in het verleden tot weinig andere keuzes geleid heeft, is de vraag of met name risico's rondom leveranciersafhankelijkheid, autonomie en weerbaarheid goed ingeschat zijn. Op basis van de recente ontwikkelingen en nadruk vanuit de politieke om deze onderwerpen te prioriteren, dient de manier waarop risico's geïdentificeerd
worden en de manier waarop de kans en impact bepaald wordt aangepast te worden. Hierbij is een holistische benadering nodig die alle risico's ten aanzien van leveranciersafhankelijkheid, autonomie en weerbaarheid in kaart brengt.

Ook is het van belang dat risicoanalyse niet als eenmalige actie uitgevoerd wordt voor het herijken van beleid, maar dat dit meer dynamisch gedaan wordt, zodat beter omgegaan kan worden met veranderingen ten aanzien van de belangrijkste risico's. Hierbij is een dashboard waarin de kans en impact op specifieke risico's en de staat van de mitigerende maatregelen is opgenomen een goed instrument om de risicostatus te monitoren. Hoewel grote veranderingen geen directe impact op de uitvoering zullen (kunnen) hebben, kan aanzienlijke wijziging in het risicobeeld leiden tot aanpassing in de langere termijnstrategie. Wijzigingen in de risicoanalyse dienen daarom gedeeld met en beoordeeld worden met het verantwoordelijke gremium voor dergelijke beleidswijzigingen. Welk gremium dit is, zal afhankelijk zijn van de organisatie.

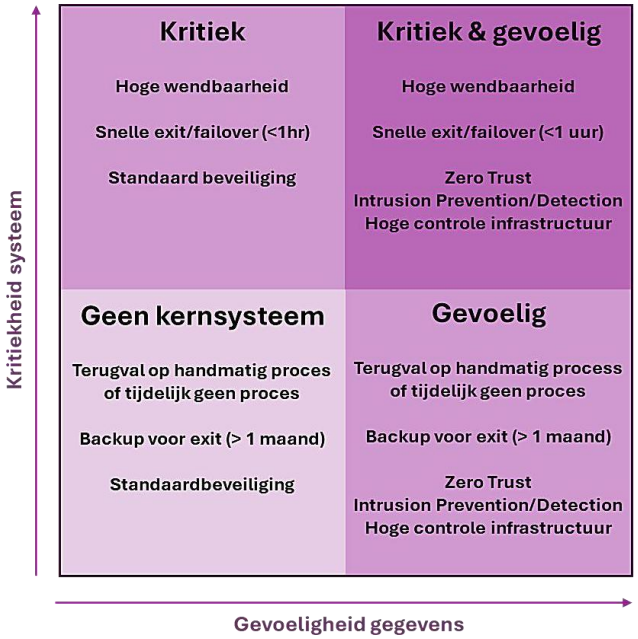
Dit rapport bevat geen uitputtende lijst van risico's met betrekking tot data-toegang en systeembeschikbaarheid, al is echter van belang om hierbij verder te kijken dan toegang tot data of het ontzeggen van toegang tot diensten door de Amerikaanse overheid. Vanuit aanleiding dient de volgende lijst bedreigingen als goed startpunt:

- Toegang tot data door een buitenlandse mogendheid via
  - Hackpogingen van zogenaamde Nation State Actors, natiegedreven hackers collectieven;
  - Gerechtelijk bevel op basis van wetgeving rondom crimineel onderzoek (bijvoorbeeld CLOUD Act);
  - Gerechtelijk bevel op basis van wetgeving rondom (contra) spionage (bijvoorbeeld FISA).
- Toegang tot data door kwaadwillenden via
  - Hackpogingen (bijvoorbeeld door criminele organisaties);
  - Interne actoren.
- Niet meer beschikbaar zijn van data/systemen door
  - Menselijke fouten
  - Randsomware aanval;
  - Exorbitante prijsverhoging van toeleveranciers van o.a. hardware en software;
  - Niet meer beschikbaar zijn van de Leverancier, bijvoorbeeld door failissement;
  - Gerechtelijk bevel (bijvoorbeeld Executive Order door Amerikaanse president);
  - Natuurlijke ramp;
  - Oorlog.

2.1.2 Portfolio analyse

De impact van de risico's is niet hetzelfde voor ieder systeem. Het is daarom van belang om een portfolio analyse uit te voeren waarin systemen gegroepeerd worden aan de hand van de organisatiedoelstellingen en de voor de betreffende systemen toepasselijke risico's ten aanzien van het behalen van die doelstellingen. Voor autonomie en weerbaarheid kunnen systemen op verschillende manieren ingedeeld worden. De overheid zou hier een uniforme manier van classificatie voor moeten gebruiken op basis van de NDS, om vervolgens aan de verschillende classificaties mitigerende maatregelen te koppelen.

Als voorbeeld wordt hieronder een methodiek besproken rondom classificatie en daaraan te koppelen maatregelen. Hierbij worden applicaties ingedeeld langs twee assen: gevoeligheid van de gegevens en hoe kritiek de functie van het systeem is. Dit kan door per scenario te bepalen of het systeem bestand moet zijn tegen dat scenario. Hoe meer scenario's gemitigeerd moeten kunnen worden, hoe hoger de score op de betreffende as. Systemen die laag op beide assen scoren, vereisen weinig mitigerende maatregelen en kunnen in principe op de meest kosteneffectieve manier gebouwd en uitgevoerd worden. Systemen die hoog scoren op beide assen zullen ontworpen, gebouwd en geopereerd dienen te worden om alle risico's adequaat af te kunnen dekken. Waarbij een afweging gemaakt dient te worden tussen verschillende non-functionele behoeftes. Zo spelen naast de risico's ook zaken als functionaliteit en kosten een rol. De onderstaande afbeelding geeft een voorbeeld van de groepering bij een portfolio analyse.



Figuur 2 : Voorbeeld groepering bij een portfolio analyse

2.1.3 Oplossingsarchetypen definiëren

Op basis van de portfolio analyse kunnen voor verschillende groepen systemen archetypen worden gedefinieerd, die bepalen hoe deze systemen ontworpen, geïmplementeerd en geopereerd worden. De archetypen maken het mogelijk om de organisatie in te richten voor een beperkte set aan technologieën en operatiemodellen, waardoor gestuurd kan worden op organisatiestructuur, de nodige expertise en efficiency. Voor de archetypen dienen minimaal de volgende zaken duidelijk te zijn:

- Wat is nu en in de toekomst van de rol van de applicatie in (kritieke) processen en hoe verandert dit mogelijk. Het 7R framework zoals besproken in 2.3.3.2 Oplossingsstrategie en business case bepalen is een goed framework om dit te bepalen.
- Architectuur van de systemen
  - Welke eisen worden gesteld aan hoe het systeem ontworpen wordt/is ten aanzien van type infrastructuur (bijvoorbeeld virtuele machines, containers, PaaS diensten)?
  - Welke eisen worden gesteld aan de technologie die gebruikt wordt bij de ontwikkeling of selectie van systemen?
  - Welke beveiligingseisen worden gesteld aan het systeem? Dit betreft zowel fysieke beveiliging als logische beveiliging middels identiteits- en toegangsbeheer, encryptie, intrusie detectie en de Secure Software Development Lifecycle.
- Bedrijfscontinuïteit en leveranciersafhankelijkheid
  - Welke methodes moet het systeem implementeren voor bedrijfscontinuïteit? Denk hierbij aan zaken als opereren in meerdere datacentra of multi-cloud, de manier van failover en backup.
  - Is een exit-strategie nodig en welke eisen moeten daaraan gesteld worden? Hoe snel moet een exit mogelijk zijn en wat betekent dit voor bijvoorbeeld opslag en transport van (grote volumes) gevoelige data?
  - Onder wat voor bedrijfscontinuïteitsscenario's mag afgeweken worden van beveiligingsbeleid van systemen met gevoelige data?
- Ontwikkeling en operatie
  - Welke expertise is nodig op het gebied van ontwikkeling/implementatie en operatie van de systemen, en hoe wordt dit geborgd in de organisatie?
  - Hoe werken verschillende teams in de organisatie samen om systemen succesvol

te ontwikkelen/implementeren en vervolgens te opereren?
- Leveranciersmanagement
  - Wat zijn de eisen die gesteld worden aan leveranciers en aan contracten? Hieronder vallen alle zaken in scope die van toepassing kunnen zijn, zoals datacentra, hardware, software en diensten.

Architectuur van systemen

Applicaties opdelen in groepen maakt het mogelijk om uniforme eisen te stellen aan bijvoorbeeld het exit-plan en deze om te zetten in architectuurkeuzes waarbij componenten en processen geüniformeerd kunnen worden om aan deze eisen te voldoen. Zelfs tussen groepen kunnen uniforme keuzes gemaakt worden om nog meer profijt te hebben van standaard ontwikkel- en operatiemodellen.

Het is hierbij aan te bevelen om zoveel mogelijk in te zetten op moderne “cloud native” architecturen, omdat die een hoge mate van abstractie hebben van de onderliggende infrastructuur, waardoor het makkelijker is om deze te verhuizen naar andere infrastructuur. Het is daarbij wel van belang dat er goed gebruik gemaakt wordt van de mogelijkheden die cloud native ontwikkeling biedt om te abstraheren van veelgebruikte componenten voor bijvoorbeeld dataopslag, beveiliging en messaging. Dat maakt het mogelijk om daarvoor PaaS diensten toe te passen zonder dat daarop een afhankelijkheid ontstaat. Dit moet terugkomen in ontwikkelprincipes, maar ook in de selectie van softwarepakketten.

Het bovenstaande is voor nieuwbouw een stuk makkelijker te realiseren dan voor bestaande applicaties, zeker als deze aangekocht zijn en hele specifieke functionaliteit bieden. Als dergelijke systemen daardoor niet kunnen voldoen aan bepaalde eisen van een groep binnen de portfolio, is het belangrijk om een plan te maken voor de langere termijn om te bepalen hoe daarmee omgegaan wordt.

Bedrijfscontinuïteit en leveranciersafhankelijkheid

Voor de bouw of aanschaf van nieuwe systemen, of het moderniseren van bestaande systemen, kunnen principes gehanteerd worden die zorgen voor minder afhankelijkheid van leveranciers en meer flexibiliteit voor het opereren van de systemen zodat bedrijfscontinuïteit en exit-scenario’s eenvoudiger te realiseren zijn (Figuur 3).

Open standaarden

Bij voorkeur worden voor systemen open standaarden gebruikt. Dergelijke standaarden, zoals ontwikkeld door ISO/IEC, ECMA en W3C kunnen ondersteund worden door meerdere leveranciers en/of open source initiatieven. De ondersteunde functionaliteit en het gebruiksgemak kan per oplossing verschillen.

De facto standaarden

Daar waar open standaarden niet beschikbaar zijn, kan gebruik gemaakt worden van de facto standaarden, meestal gebaseerd op open source van bijvoorbeeld de Apache Foundation, Eclipse Foundation, Linux Foundation en Cloud Native Compute Foundation (CNCF).

Figuur 3: Volgorde van principes die gehanteerd kunnen worden bij de bouw of aanschaf van nieuwe systemen, of het moderniseren van bestaande systemen die zorgen voor minder afhankelijkheid van leveranciers en meer flexibiliteit voor het opereren van de systemen.

De Linux Foundation beheert onder andere de Open Container Initiative (OCI) wat een standaard image formaat levert voor container technologie en Jenkins (via de sub-divisie Continuous Delivery Foundation) voor de automatisering van software delivery. CNCF beheert onder andere Kubernetes voor container orkestratie en een reeks aan projecten daar omheen voor het ontwikkelen en opereren van applicaties zoals Dapr (Distributed Application Runtime) voor de abstractie van applicatie code van de onderliggende infrastructuur en de Helm package manager die het uitrollen en beheren van Kubernetes applicaties vereenvoudigt. Deze open source standaarden worden door veel hosting en cloud providers ondersteund, waardoor systemen makkelijk(er) verplaatsbaar zijn. Open source blijft ook aanpasbaar en geeft dus meer controle.

Gedragen initiatieven
Naast de facto standaarden zijn er ook andere initiatieven voor standaardisatie en open source die succesvol gebruikt kunnen worden. Daarbij is het belangrijk dat dergelijke initiatieven goed gedragen worden – bij voorkeur door verschillende partijen – en genoeg ontwikkelaars actief zijn om het onderhoud te plegen. In Europa zijn er een aantal initiatieven om technologie te ontwikkelen die het makkelijker moeten maken om gegevens uit te wisselen en infrastructuur op een uniforme manier aan te sturen, zoals Gaia-X (“soevereine” data uitwisseling), IPCEI-CIS (cloud technologie), en SECA (standaard API voor cloud providers, gedreven door EuroStack). Verder zijn er ook Europese bedrijven die open source ontwikkelen, wat inhoudt dat de technologie in principe vrij te gebruiken is, maar waarbij de leverancier een ondersteuningsmodel biedt.
Proxmox en OpenNebula, die zijn opgenomen in dit rapport, zijn daar voorbeelden van.

“Wendbare” leverancierseigen technologie
Verder is er “wendbare” leverancierseigen technologie (technologie waarvan een specifieke leverancier de eigenaar is, ook wel “proprietary” genoemd) die op veel platformen werkt en/of waarvoor brede expertise aanwezig is om systemen mee te ontwikkelen en te opereren. Java en .NET zijn voorbeelden van (deels) leverancierseigen technologie waar heel veel ontwikkelaars mee kunnen werken. En bijvoorbeeld SQL Server en Oracle zijn dermate veel gebruikte databases dat ze door veel partijen geopereerd kunnen worden. Bij het wegvallen van de leverancier zal op den duur wel gezocht moeten worden naar alternatieven, waarbij te verwachten is dat er een behoorlijke community zal zijn die alternatieven en migratie tools zal ontwikkelen (voor zover niet al beschikbaar). Hoewel deze technologie als laatste overwogen zou moeten worden bij het bouwen of aanpassen van systemen, is het niet per definitie zo dat deze technologie ongeschikt is vanwege de herkomst van een bepaalde leverancier.

Leverancierseigen technologie
Pas als laatste dient gekeken te worden naar leverancierseigen technologie die niet (of in beperkte mate) wendbaar is. Deze zou in principe vermeden moeten worden, maar kan nodig zijn omdat het sleutelfunctionaliteit betreft. Voorbeelden van dergelijke technologie betreft SAP en VMware, die wanneer deze eenmaal geïmplementeerd zijn niet eenvoudig te vervangen of verplaatsen zijn, omdat ze meestal kernfuncties leveren op een grote schaal. Voor een systeem als SAP wordt dit veroorzaakt doordat processen in de organisatie ingericht worden op hoe de software daarmee omgaat en andersom doordat de softwareconfiguratie specifiek gemaakt wordt voor de processen in de organisatie. Voor een systeem als VMware is de manier waarop het rekenkracht-, opslag- en netwerkdiensten levert specifiek gekoppeld aan de tooling rondom het systeem en is er geen enkele leverancier die dit identiek oplost en daarmee eenvoudig over te nemen maakt.

Ontwikkeling en operatie
Systemen flexibeler maken vereist hetontwikkelen of selecteren volgens specifieke principes. Dit vergt in veel gevallen ook andere expertises, bijvoorbeeld over:

- Hoe sterk bepaalde standaarden zijn en hoe deze geïmplementeerd worden door verschillende leveranciers, zodat ingeschat kan worden hoe een overstap naar een andere leverancier werkt.
- Het kunnen werken met standaardenorganisaties om standaarden te verbeteren.
- Andere ontwikkelprocessen en architecturen, zoals Cloud Native ontwikkeling op basis van containers.
- Hoe ontwikkeld moet worden met open source en hoe ondersteuning daarin werkt.
- De interne werking van belangrijke open source software, zodat deze door de eigen organisatie gecontroleerd en aangepast kan worden. Ongeveer 80% van de open source contributies komen van buiten Europa. Het is daarom van belang dat aanpassingen niet zomaar overgenomen worden en er eventueel kennis is om zelf wijzigingen door te voeren. Een deel van het software supply chain risico kan gemitigeerd worden door gebruik te maken van ondersteunde open

source software. Dit is software waarbij een leverancier zorgdraagt voor het controleren en zo nodig integreren van software voor eenvoudiger gebruik. Voorbeelden hiervan zijn Red Hat en Suse die Linux en Kubernetes leveren.
- Het bijdragen aan open source initiatieven om deze beter geschikt te maken voor de eisen van de organisatie.

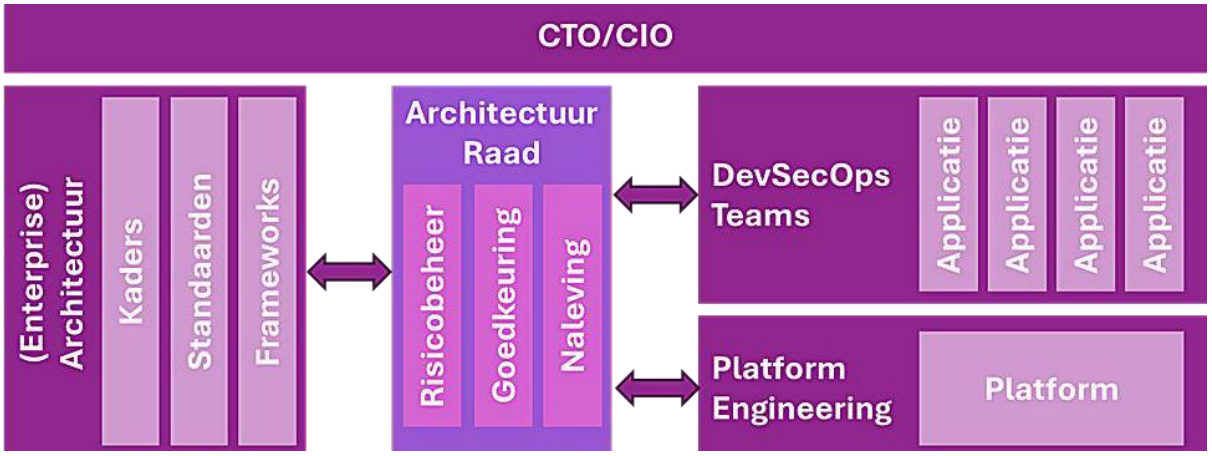
Ook voor de operatie brengt dit veranderingen met zich mee, omdat het platform dat beheerd moet worden uit andere en mogelijk meer technologieën bestaat en de ondersteuning vanuit de leverancier anders kan zijn dan voorheen. Hoewel het (virtualisatie)platform mogelijk al centraal beheerd wordt, sluit de adoptie van Platform Engineering aan op de veranderende eisen. Daarin kan ook geborgd worden dat sommige onderdelen van het platform vereisen dat er expertise aanwezig is binnen de organisatie om platform software aan te passen. Platform Engineering gaat hand in hand met applicatieontwikkeling op basis van DevSecOps, wat gezien wordt als de moderne manier van het ontwikkelen en opereren van software.

Als die zaken geen onderdeel uitmaken van het standaardcontract, moet dit vooraf onderhandeld worden.

2.1.4 Organisatiestructuur en processen

De overgang naar een IT organisatie waarin platformen centraal beheerd worden en applicaties ontwikkeld en beheerd worden via DevSecOps teams, vraagt om een fundamentele herinrichting van structuur, rollen en processen. Dit model sluit aan op de strategische uitgangspunten zoals beschreven in dit rapport, waarbij autonomie, wendbaarheid, flexibiliteit en verkleining van leveranciersafhankelijkheid centraal staan.De organisatie bestaat uit drie hoofdcomponenten:

1. Platform Engineering – verantwoordelijk voor het ontwerpen, bouwen en beheren van de gemeenschappelijke platformen waarop applicaties landen.
2. DevSecOps teams – multidisciplinaire productteams met end to end verantwoordelijkheid voor applicaties.
3. Centrale governance structuur – voor kaders, compliance, architectuur, risicobeheer en strategische besluitvorming.



Figuur 4: Overzicht organisatiestructuur van een IT organisatie waarin platformen centraal beheerd worden en applicaties ontwikkeld en beheerd worden via DevSecOps teams

Leveranciersmanagement

Daar waar architectuurkeuzes ook naar leveranciers toe technische eisen stellen aan de oplossing, is leveranciersmanagement de manier om te zorgen dat ook contractueel leveranciers aan de eisen kunnen voldoen. Als een snelle verhuizing nodig is van een groep applicaties, is het bijvoorbeeld van belang dat de licentiestructuur dit ondersteunt. En als een leverancier niet meer aan bepaalde eisen voldoet, moet het mogelijk zijn om zonder- of tegen beperkte boete een exit te maken en wellicht zelfs ondersteund te worden met expertise.

Deze organisatiestructuur is niet afhankelijk van het gebruikte platform en kan ook toegepast worden met een bestaand platform, indien dat platform de mogelijkheden biedt om de juiste afbakeningen te verzorgen tussen teams. Wat kan verschuiven bij het adopteren van een ander platform is het type diensten dat geleverd kan worden door het Platform Engineering team en de mate van automatisering die dit mogelijk maakt.

Platform Engineering

Het platformteam levert betrouwbare, veilige en gestandaardiseerde kerndiensten (compute, netwerk, virtualisatie, containers) waarop DevSecOps teams zelfstandig kunnen opereren. Dit wordt gedaan op basis van zogenaamde “landing zones” waarbinnen DevSecOps-teams op basis van “selfbediening” applicaties kunnen uitrollen en uitgevoeren binnen opgezette kaders. Dit vereist een hoge mate van automatisering, inzicht in wat er in het platform gebeurt (observability), en voorzieningen voor lifecycle management en continue kunnen uitrollen van applicaties (CI/CD).

Het valt buiten de scope van dit rapport om uitgebreid in te gaan op het opzetten van een Platform Engineering team, maar belangrijke principes voor Platform Engineering zijn:

- Zoveel mogelijk automatiseren met “Everything-as-Code” (infrastructuur, policies, configuraties en pipelines worden declaratief beheerd), pipelines en GitOps.
- Een robuuste security opzet op basis van Identity & Access Management en Zero Trust principes.
- Goede monitoring en incident afhandeling op basis van interne Service Level Objectives (SLO) en naar de afnemers gerichte Service Level Agreements (SLA).
- Product-thinking, waarbij elk platformonderdeel een backlog en een product owner heeft die zorgt dat de SLO en SLA gehaald worden.

DevSecOps teams

DevSecOps teams zijn verantwoordelijk voor:

- Ontwikkeling, testen, beveiliging, uitrollen en opereren van applicaties.
- Het naleven van centrale kaders (architectuur, beveiliging, lifecycle policies).
- Het zelfstandig uitrollen van applicaties via self service tooling van het platform.
- Het beheren van de volledige lifecycle van applicaties.

Dit sluit aan bij een moderne manier van ontwikkelen en opereren van applicaties. DevSecOps brengt development, security en operations in één cyclisch proces samen.

Het valt buiten de scope van dit rapport om uitgebreid in te gaan op het opzetten van een DevSecOps cultuur en teams, maar in de kern werkt DevSecOps rond het continue uitrollen van nieuwe versies van applicaties (Continuous Integration & Deployment of CI/CD), waarbij beveiligingscontroles automatisch uitgevoerd worden tijdens het uitrolproces. Kwaliteitscontrole en geautomatiseerd testen speelt daarom ook een belangrijke rol binnen DevSecOps.

Governance structuur

Platform Engineering en DevSecOps dienen goed op elkaar aan te sluiten, waardoor een governance structuur nodig is die zorgt voor duidelijke strategische besluitvorming, risicobeheer, en naleving van kaders en architectuur. Naast de CIO en CTO is hierbij een belangrijke rol weggelegd voor Enterprise Architecture voor het vaststellen van de frameworks en standaarden, en het toezien op de naleving daarvan middels goedkeuringsprocessen in een architectuur gremium waarin ook een afvaardiging zit van Platform Engineering en de DevSecOps organisatie.

2.1.5 Ecosysteem ontwikkeling

Zoals eerder besproken is het onrealistisch voor de overheid om alles zelf te kunnen, en bovendien niet nodig zolang de benodigde capaciteiten in de markt aanwezig zijn. De afhankelijkheid op niet-Europese leveranciers is daarbij momenteel wel hoog, en voor betere autonomie is een sterker Europees en Nederlands ecosysteem nodig. Bij de samenwerking tussen overheidsorganisaties kan een meer expliciete keuze voor Europese en Nederlandse oplossingen bijdragen aan het verbeteren van het ecosysteem waar in de overheid zowel haar eigen expertise ontwikkelt als richting geeft aan de markt.

Waar dit niet al gebeurt, kan dit door duidelijk te maken welke capaciteiten nodig zijn, zodat de Europese en nationale markt naar de behoefte van de overheid toe kan ontwikkelen. Dit betekent dat bij aanbestedingen toekomstige behoefte beschreven moet worden, waarbij de beoordeling deels plaatsvindt op het plan om over een bepaalde periode tot specifieke doelen te komen. Dit biedt zekerheid voor investeringen en verkleint het kip-ei-probleem wanneer de overheid bepaalde capaciteiten wenst die binnen Europa nog niet beschikbaar zijn.

2.2 Verminderen van leveranciersafhankelijkheid

De in 2.1 Strategische aanpak autonomie en weerbaarheid beschreven aanpak zorgt op strategisch niveau voor minder leveranciersafhankelijkheid. Op een meer tactisch niveau hebben organisaties een aantal mogelijkheden om leveranciersafhankelijkheid te verminderen:

- Exit onderdeel maken van leverancierselectie
- Meerdere leveranciers naast elkaar gebruiken
- Open standaarden kiezen
- Open source toepassen

2.2.1 Exit onderdeel maken van leverancierselectie

Door een toekomstige exit onderdeel te maken van de leverancierselectie kan een duidelijke inschatting gemaakt worden van de impact die een exit met zich meebrengt en kan dit meewegen in de selectie. Zelfs als gebruik gemaakt wordt van open standaarden is het niet vanzelfsprekend dat een exit eenvoudig te realiseren is en daarom dient gekeken te worden naar:

- Welke alternatieven beschikbaar zijn.
- Hoe dichtbij alternatieven liggen qua functionaliteit en gebruiksgemak.
- Hoe een exit-/migratieplan eruitziet en welke tijdlijnen mogelijk zijn.
- Welke tooling beschikbaar is voor migratie naar alternatieven.

Dit betekent niet dat een geheel uitgewerkt exit-plan beschikbaar moet zijn als onderdeel van de leverancierselectie. Er moet echter genoeg inzicht zijn in wat de impact is om dat mee te kunnen wegen. Nadat een leverancier geselecteerd is, dient als onderdeel van de implementatie wel een volledig exit-plan gemaakt te worden. Dit plan dient ook periodiek bijgewerkt te worden om te zorgen dat een exit daadwerkelijk uitgevoerd kan worden.

2.2.2 Meerdere leveranciers naast elkaar gebruiken

Daar waar het binnen een organisatie mogelijk is om bepaalde functionaliteit te segmenteren, kan ervoor gekozen om voor verschillende segmenten dezelfde functionaliteit door verschillende leveranciers te laten leveren, bijvoorbeeld verschillende virtualisatieplatformen of verschillende communicatieplatformen. Daarmee heeft de organisatie van meerdere platformen kennis in huis en is het dus mogelijk om te bewegen tussen die platformen. Vermindert de levensvatbaarheid van een van de platformen, dan kan gedeeltelijk of geheel overgestapt worden naar een ander platform, omdat de expertise aanwezig om die overstap te maken. Als daardoor nog maar één platform overblijft, zal een selectie gestart moeten worden voor een secundair platform. Het team dat verantwoordelijk was voor het oude platform kan dan omgeschoold worden voor het nieuw te selecteren platform, waardoor de organisatorische impact beperkt is.

Dat er gebruik gemaakt kan worden van beschikbare expertise en organisatorische impact in veel gevallen beperkt blijft tot omscholing, betekent niet dat een overstap naar een aanwezig platform zonder impact is:

- De onderliggende hardware moet hergebruikt kunnen worden door het (meer) te gebruiken platform (doelplatform) of er is nieuwe hardware nodig.
- Licenties voor het doelplatform moeten worden uitgebreid en licenties voor het oorspronkelijke platform (bronplatform) moeten afgeschaald worden.
- Configuratie die ingeregeld was in/voor het bronplatform voor de applicaties die daarop functioneerden moet overgezet worden.
- Beheerders van het bronplatform moeten (deels) omgeschoold worden naar het doelplatform.
- Afhankelijk van hoe de platformen binnen de organisatie beheerd werden, kan een wijziging nodig zijn in de organisatie. Dit kan beperkt zijn tot een aantal mensen dat verschuift van een organisatieonderdeel naar een ander, maar kan ook verdere gevolgen hebben.

Meerdere platformen naast elkaar opereren maakt de onderhandelingspositie sterker bij het heronderhandelen van een contract, omdat de keuze er is om een ander platform uit te breiden. Het verschuiven van een platform naar een ander tijdens een lopend contract, kan echter wel negatieve gevolgen hebben voor de kosten en kan ook tot contractbreuk leiden. Het is daarom belangrijk dat bepaalde exit-scenario's in het contract opgenomen zijn.

Een ander aandachtspunt is dat meerdere platformen naast elkaar opereren als nadeel heeft dat dit een zekere mate van overhead met zich meebrengt in de operatie. Ten eerste is kennis nodig van meerdere platformen en dit betekent in de meeste gevallen meer mensen en/of meer opleidingskosten. Ten tweede kan het afhankelijk van het type functionaliteit betekenen dat er een zekere mate van overhead is in de hoeveelheid infrastructuur die nodig is. Tot slot zijn leveranciers geneigd om hogere kortingen te geven naarmate een organisatie meer afneemt. Meerdere kleinere platformen

kunnen daardoor minder profijt hebben van kortingen. Het is dus niet per definitie zo dat het voor iedere organisatie dit de juiste oplossing is. Er moet goed gekeken worden dat de toegevoegde complexiteit in verhouding staat met het probleem dat opgelost moet worden. De complexiteit kan verlaag worden door de keuze te maken voor een automatiseringsplatform dat een generieke interface biedt over meerdere clouds.

2.2.3 Open standaarden kiezen

Een open standaard is een implementatiestandaard die door meerdere leveranciers wordt ondersteund en toegepast. Het gebruik van open standaarden is een belangrijke voorwaarde voor wendbaarheid, omdat het organisaties in staat stelt om te kiezen tussen zowel commerciële ("proprietary") als open source oplossingen zonder direct een sterke afhankelijkheid van één specifieke leverancier te creëren.

Het is daarbij van belang om open standaarden en open source nadrukkelijk te onderscheiden. Open standaarden gaan over uitwisselbaarheid, interoperabiliteit en portabiliteit; open source gaat over het licentiemodel en de beschikbaarheid van broncode. Open standaarden kunnen dus worden gerealiseerd met zowel closed source als open source oplossingen. Voor het beperken van vendor lock-in is het hanteren van open standaarden daarom het primaire ontwerpprincipe.

Open standaarden kunnen op verschillende manieren tot stand komen. Ze kunnen officieel zijn vastgelegd door erkende standaardisatieorganisaties, maar ook de facto standaarden zijn, die door brede adoptie in de markt feitelijk als standaard functioneren. Een bekend voorbeeld hiervan is de OCI Container Standard, die ervoor zorgt dat containers op een gestandaardiseerde manier worden verpakt en uitgevoerd. Hierdoor wordt de portabiliteit van containers tussen verschillende containerplatformen en leveranciers gewaarborgd.

Het toepassen van open standaarden draagt direct bij aan het verminderen van vendor lock-in. Wanneer systemen en platformen zijn gebaseerd op algemeen geaccepteerde standaarden, wordt een toekomstige overstap naar een ander platform of een andere leverancier aanzienlijk eenvoudiger. Dit maakt de exitstrategie minder complex, omdat het migratiepad beter voorspelbaar is en minder maatwerk vereist. Tegelijkertijd blijft het noodzakelijk om expliciet een exitstrategie te definiëren en vast te leggen; het gebruik van open standaarden neemt deze noodzaak niet volledig weg.

Daarbij is het belangrijk om kritisch te blijven op het gebruik van leveranciersspecifieke uitbreidingen, opties of add-ons. Deze functionaliteiten worden vaak door leveranciers aangeboden als onderscheidend vermogen ten opzichte van concurrenten, maar kunnen leiden tot nieuwe afhankelijkheden. Wanneer dergelijke specifieke features diep in de oplossing worden geïntegreerd, kan dit de overstap naar een alternatief platform alsnog bemoeilijken en de voordelen van het gebruik van open standaarden deels tenietdoen.

2.2.4 Open source toepassen

Open source software heeft als voordeel dat het eigenaarschap van de broncode in het publieke domein ligt. Er is daarmee minder afhankelijkheid op een specifieke leverancier, want het is immers mogelijk om zelf de code aan te passen als dit nodig is. Het is echter te simpel om te denken dat hiermee alle afhankelijkheid vervalt, aangezien er weldegelijk een afhankelijkheid is op mensen die de software onderhouden terwijl daar geen contractuele afspraken mee zijn. We kunnen grofweg drie verschillende vormen van open source onderscheiden:

- **De facto standaarden** – door een non-profit organisatie beheerde open source waarbij meerdere (grote) softwareleveranciers bijdragen aan verbeteringen. De zekerheid dat deze software doorontwikkeld blijft worden is hoog.
- **Gedragen initiatieven** – meestal gedreven door een non-profit organisatie met meerdere partijen die bijdragen, maar niet op de schaal van de facto standaarden. Het succes van deze software is niet gegarandeerd en kan op langere termijn een risico vormen.
- **Individuele initiatieven** – gedreven door één organisatie of een groepje mensen dat een bepaald probleem wil oplossen. Het bestaansrecht van deze software hangt af van de welwillendheid van mensen om hun (vrije) tijd te besteden aan de doorontwikkeling en of een organisatie levensvatbaar is, hetzij door subsidie, hetzij door een commercieel beheermodel.

Zeker complexe software vergt nogal wat expertise van hoe deze software werkt.

Het proces van robuuste softwareontwikkeling is daarbij minstens zo belangrijk. Voor de facto standaarden is dit over het algemeen goed geregeld en kan een organisatie die gebruik wil maken van die software ervan uitgaan dat de doorontwikkeling goed en met genoeg controle plaatsvindt. Dat is belangrijk, omdat bij open source mensen ook malafide wijzigingen kunnen maken als daar niet voldoende controle op is.

Een ander aspect is dat bij de facto standaarden er genoeg opties zijn om een onderhoudscontract af te sluiten bij partijen met de nodige kennis en daarmee te ondervangen dat er geen verantwoordelijke leverancier is. Bij gedragen initiatieven of individuele initiatieven kan die mogelijkheid er ook zijn, maar is dit vaak maar beperkt tot een enkele partij die ondersteuning biedt. Tenzij daaromheen een afdoende ecosysteem van bijdragers is, levert dit een risico op voor de continuïteit van de ondersteuning.

Wanneer bepaalde open source software zeer belangrijk is voor een organisatie, loont het de moeite om zelf toe te treden tot het ecosysteem dat de software verder door ontwikkelt, om zo expertise op te bouwen die nodig is indien de ondersteuning door anderen wegvalt. Eventueel kan dit in samenwerking met andere overheidsorganisaties middels een (virtueel) expertisecentrum.

Wanneer het niet mogelijk is om dergelijke expertise zelf te ontwikkelen, blijft afhankelijkheid op partijen die ondersteuning kunnen bieden. De grotere leveranciers zoals Red Hat en Suse leveren hierbij open source gebaseerde software, waarin sommige componenten leverancier-eigen zijn. Bij een exit naar een van de andere open source opties, is het dan nodig om de leverancier-eigen componenten te vervangen, of om gebruik daarvan te beperken bij reguliere operatie.

2.3 Selectie en implementatie virtualisatie platform

De meeste organisaties hebben een bestaande virtualisatie platform en zullen in voorbereiding op het verlopen van bestaande contracten een selectie- en implementatieproces moeten doorlopen. Omdat het implementatieproces van een nieuw platform behoorlijk ingrijpend kan zijn en een doorlooptijd kan hebben van 6-24 maanden (en eventueel meer wanneer een andere oplossingsstrategie gekozen wordt), dient dit proces ruim voor het verlopen van contracten in gang gezet worden. In dit proces zal een keuze gemaakt moeten worden voor een van de hoofdopties:

- **Optimalisatie** van de huidige omgeving om licentiedruk te verminderen.
- **Andere leverancier kiezen** die beter aansluit op de eisen en wensen van de organisatie.
- **Meerdere leveranciers kiezen** om zo de afhankelijkheid van een enkele leverancier te verminderen.
- **Open source selecteren**, in de meeste gevallen met ondersteuning door een derde partij (leverancier).

Welke optie het beste aansluit op de organisatie hangt af van de strategische doelen van de organisatie en dient bepaald te worden wanneer de oplossingsstrategie bepaald wordt. We zien hierbij binnen verschillende organisaties verschillende richtingen, van optimalisatie van de huidige omgeving gekoppeld aan een specifieke leverancier tot het volledig weg bewegen. Dit is ook sterk afhankelijk van het type organisatie. Een aantal organisaties binnen de overheid zijn een soort Managed Service Provider en bieden een dienst aan andere overheidsorganisaties. Zij kunnen veel moeilijker van een bepaald platform af stappen als deze dienst aan meerdere klanten geleverd wordt. Het proces wat doorlopen moet worden is voor alle organisaties is in principe hetzelfde, maar kan desondanks tot een andere uitkomst leiden.

2.3.1 Oplossingsstrategie

Voor de oplossingsstrategie zijn twee kernoverwegingen leidend: het soort oplossing en het commerciële model. De intersectie van deze overwegingen bepaalt in grote mate welke oplossingen vanuit de strategie voorrang moeten krijgen. In Appendix C – Virtualisatieplatformen worden verschillende oplossingen besproken en onderstaand zijn deze gekoppeld aan de soorten oplossingen en commerciële modellen.

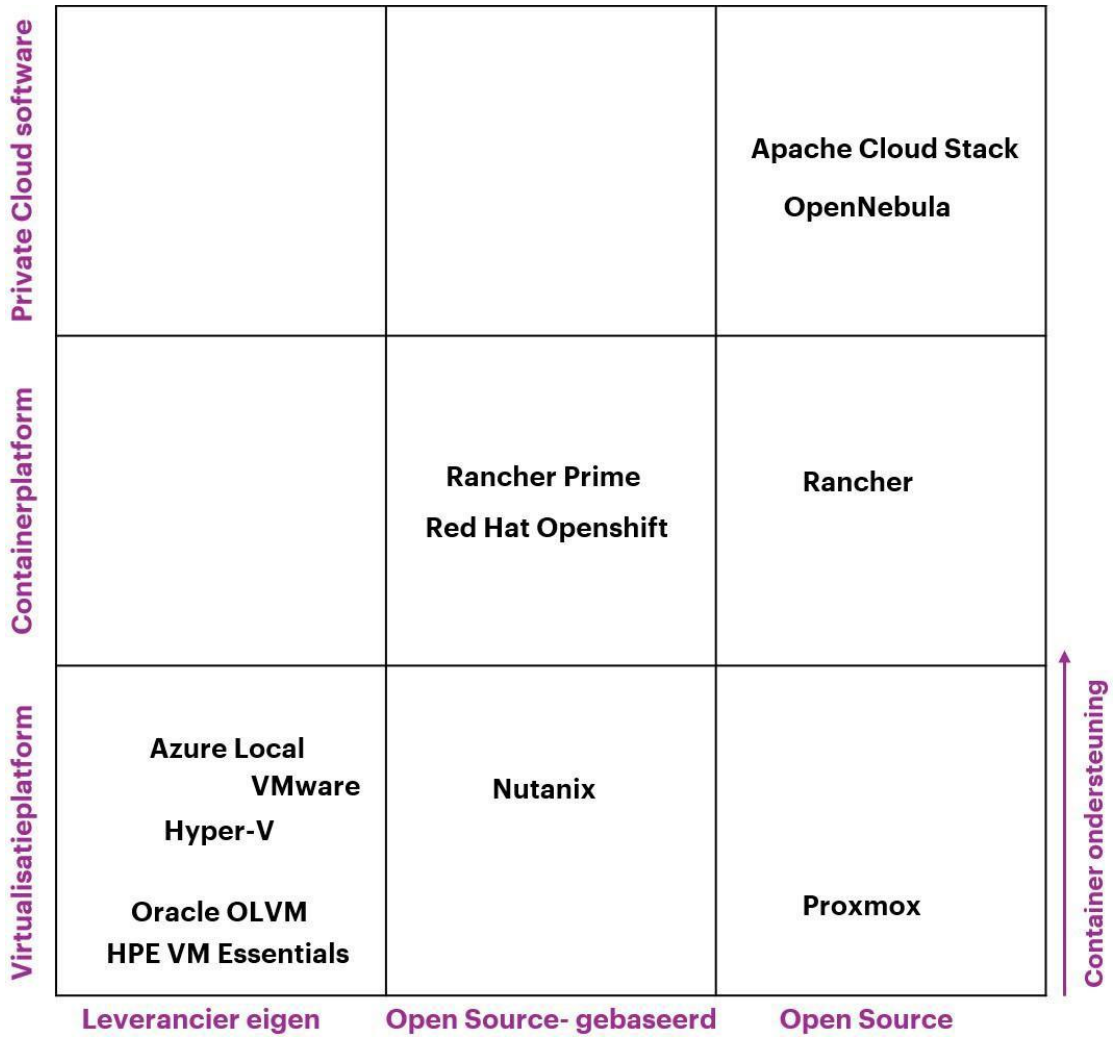
Er zijn grofweg drie soorten oplossingen te onderscheiden:

- **Traditionele virtualisatieoplossingen** waaraan containeroplossingen in meer of mindere mate toegevoegd zijn. Dit betreft HPE Morpheus VM Essentials, Microsoft Hyper-V en Azure Local, Nutanix, Oracle Linux Virtualization Manager, Proxmox en VMware.
- **Containerplatformen** waarbij ondersteuning van virtualisatie een steeds grotere rol speelt om tegemoet te komen aan de vraag om ook (nog) virtuele machines te kunnen draaien. Dit betreft Rancher en Red Hat OpenShift.

- **Private Cloud softwareoplossingen** die meerdere virtualisatieplatformen/ hypervisors ondersteunen als onderliggende infrastructuur. Dit betreft Apache CloudStack en OpenNebula.

Verder zijn er grofweg drie verschillende commerciële modellen te onderscheiden:

- **Leverancier eigen oplossingen** waarbij afhankelijkheid van de leverancier relatief hoog is, omdat migratie naar een ander platform altijd verandering met zich meebrengt naar een andere technologie. Een voordeel van deze oplossingen is dat de ondersteuning van de leverancier vaak goed is, waardoor de eigen organisatie minder expertise hoeft op te bouwen. Dit betreft HPE, Microsoft, Nutanix, Oracle en VMware
- **Volledig open source oplossingen** waarmee geen afhankelijkheid is op een specifieke leverancier. Hierbij is een organisatie vooral aangewezen op hoe actief ontwikkeld wordt door de organisatie(s) die de oplossing dragen en het ecosysteem daaromheen. Een groot nadeel van deze oplossingen is dat de levensvatbaarheid sterk afhankelijk is van het ecosysteem en dat eigen expertise opbouwen hiervoor onontbeerlijk is, met significante impact op de organisatie. Dit betreft Apach Cloud Stack, OpenNebula en Proxmox, Rancher (de volledig open source versie van Rancher Prime) valt hier ook onder.
- **Open source gebaseerde oplossingen** waarbij een groot gedeelte van de software open source is, maar via leverancier eigen componenten meer afhankelijkheid op de leverancier gecreëerd wordt. Migratie naar een ander platform is dan minder ingrijpend, omdat de kernfunctionaliteit beschikbaar is via een andere leverancier en als open source. In zekere zin is dit het beste uit twee werelden, aangezien er wel goede ondersteuning is vanuit de leverancier en daardoor de organisatie minder eigen expertise hoeft op te bouwen, maar de afhankelijkheid op de leverancier beperkt is. Dit betreft Rancher Prime (van Suse) en Red Hat OpenShift



Figuur 5: Overzicht van oplossingsstrategieën (soorten oplossingen vs. commerciële modellen)

2.3.2 Overzicht selectie- en implementatieproces

De selectie en implementatie van een nieuw virtualisatieplatform is een strategisch proces dat verder reikt dan louter technische keuzes. Het raakt aan governance, organisatieveranderingen en financiële afwegingen. Het selectieproces vereist een gestructureerde aanpak, inclusief het vaststellen van strategische doelstellingen op basis van de vastgestelde risico's, scopebepaling, analyse van de huidige situatie en het opstellen van een oplossingsstrategie. In vogelvlucht bestaat die aanpak uit de volgende stappen:

- Strategie en governance
  - Team samenstelling en governance structuur
  - Bepaling strategische doelen
  - Bepaling scope
- Platform selectieproces
  - Analyse bestaande situatie
    - Inventarisatie bestaande infrastructuur en applicaties
    - Inventarisatie impact op bestaande licenties
  - Oplossingsrichting en business case bepalen
    - Oplossingsstrategie bepalen
    - Besliscriteria voor platformselectie vaststellen
    - Documentatiestudie potentiële doelplatform(en)
    - Short-list potentiële doelplatform(en)
    - Beslisboom applicatie migratiescenarios vaststellen
    - Impact op processen en organisatie vaststellen
    - Total Cost of Ownership en business case vaststellen
    - Proof of Concept met short-list platform(en)
- Roadmap en aanbesteding(en)
- Pilot en implementatieproces

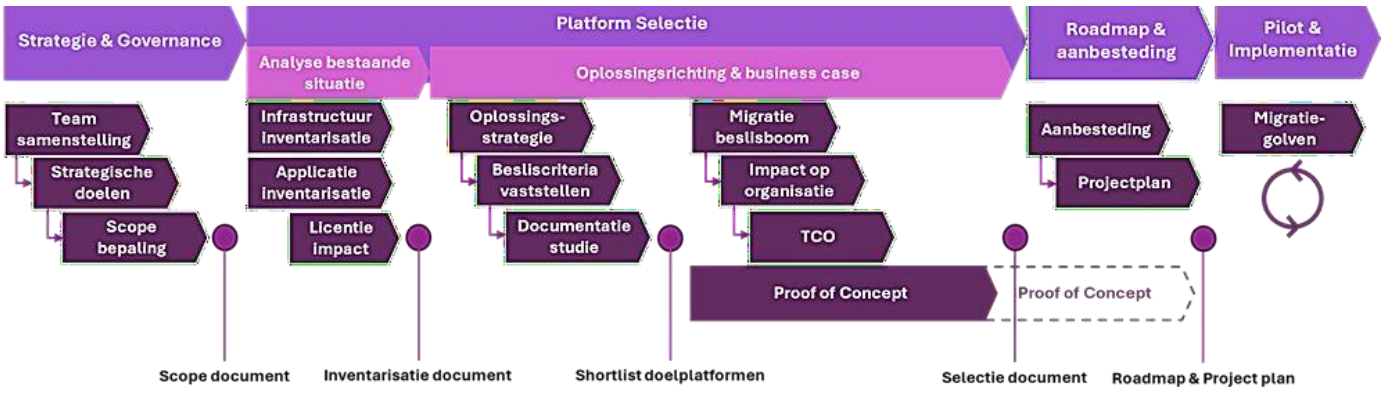
2.3.3 Strategie en governance

Team samenstelling en governance structuur

Migratie- en/of optimalisatietrajecten worden vaak beschouwd als een technische aangelegenheid. Er zijn echter andere zaken die hierbij een rol spelen, zoals de impact op bestaand IT-personeel inclusief eventuele HR-impact, financiën, en inkoop/aanbesteding. Een selectieproces om de juiste technologiekeuzes te maken is daarom niet beperkt tot de IT-organisatie, omdat deze keuzes verregaande gevolgen kunnen hebben voor hoe technologiediensten geleverd en gebruikt worden door de organisatie. Om dit goed in kaart te brengen, is het belangrijk om ook expertise uit andere delen van de organisatie te betrekken en om een governance structuur op te zetten die de juiste stakeholders zeggenschap geeft over de gemaakte keuzes. In de meest simpele vorm betekent dit dat er een uitvoeringsteam en een stuurgroep is.

Het uitvoeringsteam bestaat uit een team van technische experts uit de IT-organisatie, aangevuld met met expertise rondom sourcing, procurement, vendor management, risicobeheer en HR. Het uitvoeringsteam kan bestaan uit een kernteam, met daar omheen expertise(teams) voor verschillende deelgebieden, bijvoorbeeld voor specifieke oplossingsrichtingen.

De stuurgroep dient minimaal te bestaan uit de CIO, CTO en HR-directeur, zodat organisatiedoelen, technische doelstellingen en organisatie impact allen goed geborgd zijn.



Figuur 6: Overzicht selectie- en implementatieproces van een nieuw virtualisatieplatform

Bepaling strategische doelstellingen

Om tot de juiste keuze te komen en daar vervolgens uitvoering aan te geven zijn een aantal stappen nodig. In de eerste fase dienen allereerst de strategische doelstellingen bepaald te worden. Aangezien een overheidsorganisatie het publieke belang dient, kunnen hierbij meer factoren een rol spelen dan alleen kostenoptimalisatie, waaronder:

- Continuïteit en verbetering van dienstverlening.
- Beperken van afhankelijkheden op (niet-Europese) leveranciers.
- Stimulering van lokale of Europese technologieontwikkeling en economie.
- Verhouding tot en prioriteit van (andere) investeringsgebieden.

Deze zaken kunnen invloed hebben op de eisen die gesteld worden aan technologie, de manier waarop software en diensten gecontracteerd worden en de manier waarop contractbeheer wordt ingericht, en hoe omgegaan moet worden met vendor lock-in en exit-clausules.

Zoals gezegd zijn dit vraagstukken die niet op zichzelf beantwoord kunnen worden en daarom moeten de strategische doelstellingen niet alleen door de IT-organisatie bepaald worden. Wanneer bijvoorbeeld gekozen wordt voor een open source strategie, kan dit ook invloed hebben op de sourcing strategie. Deze keuze vereist mogelijk meer expertise binnen de organisatie, waardoor moet worden besloten of dit wordt opgevangen met eigen personeel of met inhuur van derden. De strategische doelstellingen dienen derhalve vastgesteld te worden door de stuurgroep.

Scope bepaling

De vaststelling van de scope hangt af van de strategische doelstellingen, aangezien daaruit kan volgen dat aanpalende domeinen ook dienen te veranderen. De manier waarop software ontwikkeld en geopereerd wordt kan bijvoorbeeld invloed hebben op de eisen die gesteld worden aan de mate van zelfbediening ontwikkel- en operatieteams (DevOps teams) moeten hebben en daarmee hoe zaken als opslag en netwerkbeheer ingeregeld moeten worden. De scope kan derhalve alleen de bestaande omgeving betreffen, maar het kan ook nodig zijn om andere onderdelen van het IT-landschap bij de scope te betrekken. Dit hangt ook af van de afhankelijkheden tussen componenten en de integratie tussen virtualisatie leverancier en de andere onderdelen van het IT-landschap.

2.3.4 Platform selectieproces

Analyse bestaande situatie

Na het vaststellen van de strategische doelstellingen en scope, dient de bestaande situatie in kaart gebracht te worden. Dit bestaat enerzijds uit de infrastructuur en applicaties die onder de scope vallen en anderzijds uit de impact die eventuele de licentiewijzigingen van de huidige leverancier daarop hebben.

Inventarisatie bestaande infrastructuur en applicaties

Voor de inventarisatie van de infrastructuur in scope zijn een aantal zaken van belang voor de infrastructuur die in scope valt:

- Wat is het merk/type van de infrastructuur?
- Wat is de capaciteit (CPUs/sockets, cores, hosts, opslag, netwerk capaciteit)?
- Hoe is dit onderdeel van/geïntegreerd met de infrastructuur van de virtualisatie leverancier?
- In hoeverre is de hardware herbruikbaar voor een ander platform of uniek voor het huidige platform?
- Wat is de resterende levensduur van de hardware en software?

Dit is belangrijk om vast te kunnen stellen of de bestaande infrastructuur hergebruikt kan worden of dat er nieuwe infrastructuur aangeschaft moet worden en in hoeverre dat extra afschrijving tot gevolg heeft. Voor de applicaties die in scope zijn dient het volgende vastgesteld te worden:

- Zijn de applicaties zelf ontwikkeld, ontwikkeld door een dienstverlener, of standaardsoftware?
- Wat zijn de hardware en platform vereisten van deze software?
  - Werkt de applicatie op de te optimaliseren/migreren op de infrastructuur van de virtualisatie leverancier of op andere (aanpalende) infrastructuur?
  - Wat is de CPU/geheugen/opslag vereisten?
  - Wat zijn de Operating System eisen en worden deze nog ondersteund door de leverancier?
  - Zijn er specifieke eisen zoals bijvoorbeeld Windows-clustering, Oracle RAC (Real Applications Clusters)?
- Wat is de resterende levensduur van de afzonderlijke applicaties op basis van het hardware en software platform waarop deze werk?
- Is voor elk van de applicaties de kennis aanwezig om de applicatie te blijven beheren?

Op basis van deze informatie ontstaat een overzicht van wat er in grote lijnen moet gebeuren met de applicaties, wat belangrijk is voor het bepalen van de migratiestrategie. Ook geeft dit inzicht in de eisen waaraan een doelplatform moet voldoen om de applicaties te kunnen draaien, hetgeen van belang is voor het vaststellen van de besliscriteria.

Inventarisatie impact op bestaande licenties
Om de financiële kosten en baten van de aanpak af te kunnen zetten tegen die van het blijven gebruiken van het bestaande platform, dient vastgesteld te worden wat de impact is van wijzigingen in kosten en structuur van licenties voor de bestaande omgeving, zodat een duidelijk beeld ontstaat van wat de kosten zijn wanneer het bestaande platform ongewijzigd in gebruik blijft. Hierbij is van belang wanneer een nieuw contract onderhandeld moet worden, of daarbij gebruik gemaakt kan worden van een bredere overheidsmantel, en wat de verwachtte prijsverhoging is van een nieuw contract voor de bestaande capaciteit. Daarin dient een eventueel veranderde licentiestructuur, zoals verandering naar een abonnementsmodel, meegenomen te worden.

Oplossingsstrategie en business case bepalen

Het bepalen van de oplossingsstrategie en de business case die daaruit voortvloeit bestaat uit meerdere stappen, namelijk:

- Oplossingsstrategie bepalen
- Besliscriteria voor platformselectie vaststellen
- Documentatiestudie potentiële doelplatform(en)
- Short-list potentiële doelplatform(en)
- Beslisboom applicatie migratiescenarios vaststellen
- Impact op processen en organisatie vaststellen
- Total Cost of Ownership en business case vaststellen

Hierbij gaat het zoals eerder behandeld om meer dan alleen financiële baten, aangezien de strategische doelstellingen voor andere prioriteiten kunnen zorgen.

Oplossingsstrategie bepalen – optimalisatie of migratie
Om te beginnen dient vastgesteld te worden wat de oplossingsstrategie is. Hoe het verdere proces loopt hangt af van de gekozen strategie. Zoals eerder besproken zijn de volgende strategieën mogelijk:

- **Optimalisatie** van de huidige omgeving om licentiedruk te verminderen.
- **Andere leverancier kiezen** die beter aansluit op de eisen en wensen van de organisatie.
- **Meerdere leveranciers kiezen** om zo de afhankelijkheid van een enkele leverancier te verminderen.
- **Open source selecteren**, in de meeste gevallen met ondersteuning door een derde partij (leverancier).

Indien gekozen wordt voor optimalisatie zijn de vervolgstappen beperkt tot de optimalisatie zelf en het heronderhandelen van het contract. Voor de andere opties, bepaalt of vooral ingezet wordt op een 1-op-1 vervanging of op bredere veranderingen in hoe infrastructuur en software geleverd en geopereerd worden, welke migratiescenarios van toepassing zijn.

Indien er een bestaand platform is, is de afhankelijkheid van dat platform een bepalende factor. Als er veel afhankelijkheid is van specifieke functies van dat platform – hetzij doordat deze functies door andere virtualisatieplatformen niet ondersteund worden, hetzij doordat in organisatieprocessen allerlei platformspecifieke interfaces gebruikt worden – is het niet aannemelijk dat een organisatie in korte tijd (1-2 jaar) een grootschalige migratie kan voltooien waarbij alle applicaties 1-op-1 overgezet kunnen worden naar een nieuw virtualisatieplatform. Het kan dan vanuit kostenbesparing beter zijn om te optimaliseren en ongebruikte functies die beschikbaar zijn binnen de licentie te benutten, eventueel ten koste van licenties bij andere partijen. Met name als VMware het bestaande virtualisatieplatform is, speelt dit een rol door de eerdergenoemde wijzigingen in de licentiestructuur.

Als de voordelen van het bestaande platform dermate groot zijn ten opzichte van alternatieve oplossingen en besloten wordt om het bestaande platform te behouden, dient wel een exit-strategie uitgewerkt te worden voor de mogelijkheid dat een (nood) exit nodig is.

Als ondanks de afhankelijkheid besloten wordt om naar een ander platform te migreren, zullen meerdere sporen naast elkaar moeten lopen, waarbij het bestaande platform aangehouden en in stappen verkleind wordt, terwijl het doelplatform (of doelplatformen) steeds verder uitgebouwd wordt.

Accenture onderscheidt verschillende migratiescenarios middels het 7R Framework, wat 7 scenarios bevat:

Scenario	Beschrijving	Doelplatform
Retire	Uitfaseren	Geen
Retain	Behouden op het huidige (virtualisatie) platform.	Gelijk
Rehost	Overzetten naar een ander (virtualisatie) platform.	(VM) platform
Replatform	Overzetten naar een ander (virtualisatie) platform, waarbij de applicatie overgezet wordt naar nieuwere versie van operating systeem, runtimes, databases, etc. Waar ondersteund, kan een virtuele machine ook omgezet worden in een container.	(VM) platform, Containers
Replace	Vervangen door andere (aangekochte) software of softwaredienst, waarbij verschillende doelplatformen mogelijk zijn, afhankelijk van wat ondersteund wordt.	VM platform, Containers, Cloud
Rearchitect	Herontwerp en implementatie van de applicatie met moderne technieken/technologie, met name containers.	Containers, Cloud
Reimagine	Ondersteuning van het bedrijfsproces opnieuw definiëren en nieuwe eisen implementeren.	Containers, Cloud

Figuur 7 : Accenture's 7R Framework

Als de bestaande applicaties min-of-meer in huidige staat behouden moeten worden, vallen Replace, Rearchitect en Reimagine buiten scope. Als ingezet wordt op modernisering, zijn die migratiescenario's juist erg belangrijk.

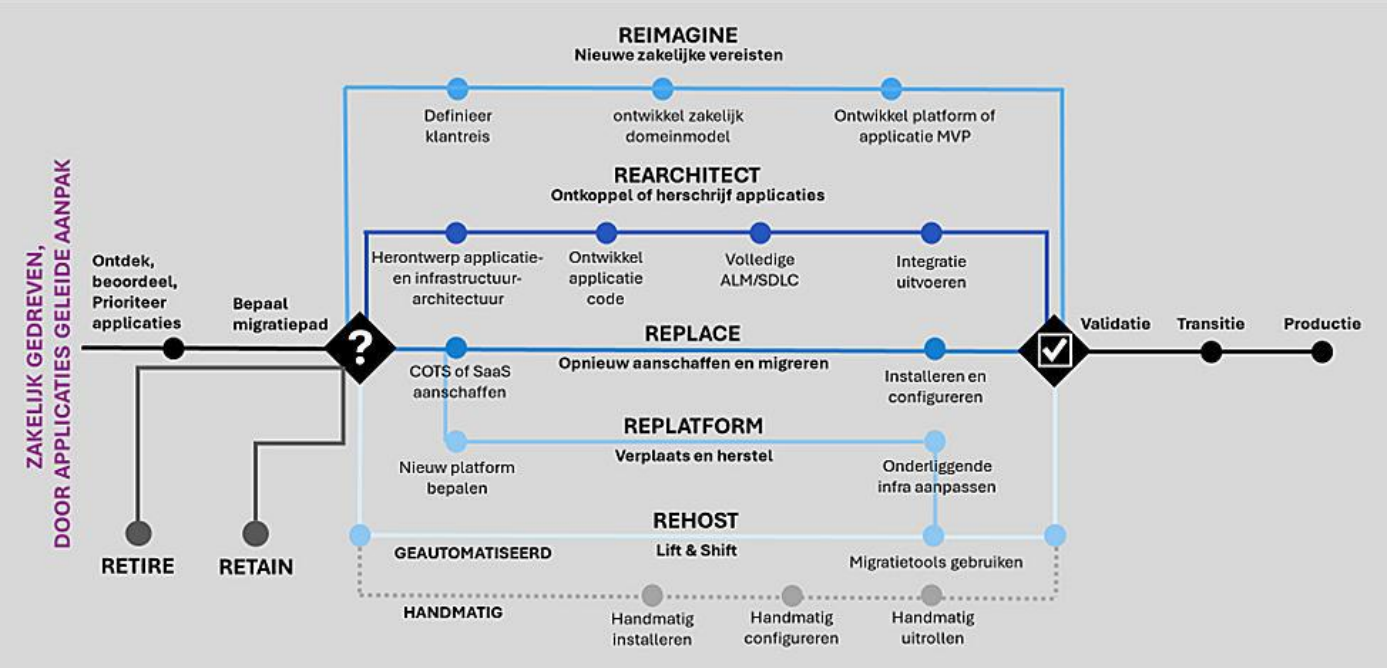
Applicatiemodernisatie is de kernvoorwaarde voor een toekomstbestendig cloud-native en infrastructuur onafhankelijk landschap. Door applicaties te moderniseren, worden zij minder afhankelijk van de onderliggende infrastructuur en platformspecifieke voorzieningen. Dit vergroot de portabiliteit, vereenvoudigt de exitstrategie en creëert meer strategische wendbaarheid, waardoor een eventuele overstap naar een ander platform in de toekomst beter uitvoerbaar wordt.

Wanneer het vooralsnog nodig is om het bestaande platform aan te houden, kan het nodig zijn om een onderscheid te maken tussen strategie voor de korte termijn en lange termijn, waarbij de langere termijn gericht is op modernisatie en het opbouwen van een nieuw platform, terwijl de korte termijn gericht is op rationalisatie van applicaties en het optimaliseren van het bestaande platform, teneinde kosten te beperken.

Het bepalen van de doelsituatie voor applicaties wordt gedaan aan de hand van een beslisboom waarin objectieve criteria zijn opgenomen om tot de juiste afweging te komen. Hierbij speelt onder andere een rol of de applicatie bedrijfsprocessen nog op de juiste manier ondersteunt, of de technologie nog levensvatbaar is (wordt deze nog ondersteund en is deze nog veilig?), en wat de kosten-baten zijn bij het aanhouden of uit faseren van de applicatie. In deze fase is deze beslisboom nog op een relatief hoog-over niveau, omdat er nog geen definitieve technologiekeuze gemaakt is. Wel zijn er een aantal belangrijke vragen die een hoog-over beeld schetsen van de eisen die applicaties hebben en die meegewogen dienen te worden bij een platformselectie:

- Welk deel van de applicaties hebben eisen hebben die vooralsnog alleen door het bestaande platform ondersteund worden?
- Welk nieuw platform of platformen zullen beschikbaar (moeten) zijn? Ligt de focus op een nieuw virtualisatieplatform of ligt de focus op het moderniseren van applicaties?
- Kunnen bepaalde soorten applicaties overgezet worden naar standaardsoftware die werkt op het toekomstige platform of een softwaredienst (Software-as-a-Service)?

Besliscriteria voor platformselectie vaststellen
In hoofdstuk 3 van dit document worden allerlei besliscriteria besproken die van belang zijn voor het maken van een keuze voor een virtualisatieplatform. Sommige van deze criteria zijn zeer specifiek ten aanzien van virtualisatieplatformen, de overige criteria kunnen ook toegepast worden op andere pakketselecties. De besliscriteria in hoofdstuk 3 dienen als startpunt voor organisaties die een ander virtualisatieplatform willen selecteren. Op basis van de eerder in het proces vergaarde informatie kunnen deze criteria verder verfijnd en aangevuld worden. Tevens kan een wegingsfactor toegekend worden, zodat de belangrijkste criteria het zwaarst wegen.



Figuur 8: Visualisatie van Accenture's 7R Framework

Het kan daarbij ook zijn dat sommige criteria worden aangemerkt als knock-out criteria, waardoor een oplossing niet verder overwogen wordt.

Documentatiestudie potentiële doelplatform(en)
Na het vaststellen van de besliscriteria kunnen de potentiële doelplatformen beoordeeld worden aan de hand van een documentatiestudie. Voor een aantal vooraanstaande platformen bevat Appendix C – Virtualisatieplatformen al een documentatiestudie voor de in dit document genoemde besliscriteria. Waar verdere criteria zijn vastgesteld dienen ook deze nog onderzocht te worden. Om tijd te besparen is het aan te bevelen knock-out criteria (waar van toepassing en waar mogelijk) als eerste te beoordelen. Platformen die afvallen door knock-out criteria hoeven dan niet op alle criteria onderzocht te worden.

Voor de documentatiestudie kan gebruik gemaakt worden van verschillende bronnen, zoals:

- Publiek beschikbare documentatie van de leverancier(s).
- Afgeschermde leveranciersdocumentatie, indien de leverancier daartoe toegang verleent
- Informatie van derden (referentiebezoeken, reviews, artikelen, forums posts, implementatiehulp, etc.).
- Kennis uit de eigen gelederen.

Tenzij binnen de organisatie kennis van alle te onderzoeken platformen beschikbaar is, is het risico op vooringenomenheid ten aanzien van een deel van de oplossingen aanwezig. Dit dient door het onderzoeksteam meegewogen te worden. Dit kan bijvoorbeeld door onafhankelijke expertise in te schakelen, informatie te vergaren van andere organisaties die al door een selectieproces zijn gegaan en besliscriteria aan te scherpen om vooringenomenheid te verminderen.

Short-list potentiële doelplatform(en)
Op basis van de documentatiestudie kan een short-list opgesteld worden met de platformen die het beste aansluiten op de strategische doelstellingen en de geformuleerde criteria. De short-list zou in principe niet meer dan 3 of 4 mogelijkheden moeten bevatten, aangezien met elk van deze platformen verdere acties nodig zijn die een aanzienlijke tijdsinvestering vergen.

Applicatie migratiescenario's verdiepen
Voor elk van de potentiële doelplatformen dient in dit stadium in meer detail duidelijk te worden wat de migratiescenario's zijn voor de verschillende applicaties. Hoewel een deel van de scenario's voor elk platform hetzelfde zullen zijn, kan het zijn dat bepaalde details ervoor zorgen dat applicaties een ander migratiescenario moeten volgen, wat weer impact kan hebben op de business case.

Om het verdiepen van de migratiescenario's uit te werken, dient de meer generieke beslisboom die eerder in het traject ontwikkeld is verder

uitgewerkt te worden voor elk van de doelplatformen. Met de beslisboom kunnen applicatieteams een beoordeling maken van het migratiescenario dat van toepassing is voor de specifieke doelplatformen.

Impact op processen en organisatie vaststellen
Het bepalen van de impact op bestaande processen en de organisatie vraagt om een gestructureerde, multidisciplinaire aanpak.

Dit begint bij het inventariseren van het huidige proces- en IT-landschap door alle bedrijfsprocessen, applicaties en infrastructuur die afhankelijk zijn van het virtualisatieplatform, en dit systematisch te documenteren. Een dependency- en traceability-analyse geeft inzicht in onderlinge afhankelijkheden tussen systemen, processen en teams. Om in kaart te brengen welke onderdelen door de migratie beïnvloed worden en waar de voornaamste risico's zich bevinden kunnen visuele modellen zoals dependency graphs ingezet worden.

Aangezien bij de invoering van een nieuw platform aanzienlijke veranderingen nodig kunnen zijn in rollen, teams en verantwoordelijkheden dient dit goed geanalyseerd te worden, waarbij aspecten als beheer, ontwikkeling, security en de benodigde competenties bekeken worden. De organisatiecultuur en veranderbereidheid van medewerkers kan de nodige frictie opleveren en het is daarom belangrijk om de organisatieonderdelen die geraakt worden te allen tijde goed geinformeerd te houden. Informeer en betrek, indien nodig, de OR tijdig bij belangrijke organisatorische veranderingen.

Total Cost of Ownership en business case(s) vaststellen
De Total Cost of Ownership (TCO) wordt berekend over een bepaalde periode. Aangezien onlangs voor een aantal overheidsorganisaties een contract met VMware afgesloten is voor een periode van 5 jaar, kan dit als maatstaf dienen voor de duur die gebruikt wordt voor de TCO-berekening. Daar moet echter wel bij aangemerkt worden dat de licentiekosten voor de periode in principe al ingeboekt zijn en dat daardoor deze organisaties ca. 5 jaar hebben om toe te werken naar de situatie na die 5 jaar.

In het geval dat alleen het gebruik van VMware geoptimaliseerd wordt, bestaat de TCO uit de operationele kosten en de infrastructuur investering. Operationele kosten (OpEx) bestaan uit de volgende onderdelen:

- Onderhoudscontracten en support voor infrastructuur
- Licenties of (onderhouds)abonnementen voor software
- Energie, koeling, facilitaire kosten
- Beheer en monitoring
- Doorlopende training en certificering
- Kosten voor compliance en security

Wanneer een migratie naar een ander platform gedaan wordt, komen hier eenmalige migratiekosten en kosten voor verandermanagement bij die voor de betreffende periode meegenomen dienen te worden:

- Voorbereiding en advies (inventarisatie, plan van aanpak, selectieproces)
- Dubbele licentie- of abonnementskosten
- Tijdelijke hardware of tooling voor migratie
- Inrichting van het nieuwe platform
- Migratie van data, applicaties en gebruikers
- Training en adoptie van medewerkers
- Kosten voor het aantrekken van extern talent indien nodig
- Verandermanagement en productiviteitsverlies tijdens transitie

Tot slot kent een migratie naar een nieuw platform ook risico's zoals projectvertragingen, downtime of dataverlies. Deze risico's dienen gekwantificeerd te worden en als voorziening opgenomen te worden in de TCO.

Proof of Concept met short-list platform(en)
Een Proof of Concept (PoC) is bedoeld om in een gecontroleerde, afgebakende omgeving te toetsen of een nieuw (virtualisatie)platform voldoet aan de functionele, technische en organisatorische eisen. Een PoC helpt om risico's te identificeren, aannames te valideren en draagvlak te creëren bij stakeholders voordat een grootschalige implementatie plaatsvindt. Uit de praktijk blijkt sommige functies die bij een documentatiestudie als voldoende gezien worden bij een PoC niet blijken te voldoen aan de eisen. Voor specifieke technische functies, zoals de performance van netwerk, opslag en functies voor bedrijfscontinuïteit, en de integratie tussen verschillende stukken infrastructuur kan dit leiden tot aanzienlijke extra kosten wanneer niet voldoende onderzocht is of die aan de eisen voldoen.

Stappenplan voor een PoC:

- Bepaal de doelstellingen: Stel vast welke functionaliteiten, prestaties en integraties getest moeten worden. Koppel deze aan de eerder opgestelde besliscriteria.

- Selecteer representatieve workloads: Kies applicaties en systemen die representatief zijn voor de productieomgeving, inclusief kritieke en minder kritieke workloads.
- Definieer succescriteria: Maak meetbare criteria voor succes, zoals performance, beheerbaarheid, integratie, security en compliance.
- Richt de PoC-omgeving in: Implementeer het platform in een gescheiden testomgeving, bij voorkeur met vergelijkbare hardware en netwerkinfrastructuur als productie.
- Voer de tests uit: Test de geselecteerde scenario's, documenteer bevindingen en vergelijk resultaten met de gestelde eisen.
- Evalueer en rapporteer: Verzamel feedback van technische teams en gebruikers, evalueer de resultaten en stel een aanbeveling op voor vervolg of aanpassing.

Voorbeelden van belangrijke types PoCs:

- Technische validatie: Test de kernfunctionaliteit van het platform, zoals virtualisatieprestaties, live migratie, storage-integratie, netwerkfunctionaliteit en ondersteuning van specifieke hardware of guest operating systems.
- Beheer en automatisering: Evalueer de beheerinterface, automatiseringsmogelijkheden (bijvoorbeeld via API's, scripting, Infrastructure-as-Code), monitoring en integratie met bestaande beheertools.
- Security en compliance: Test de mogelijkheden voor multi-factor authenticatie, role-based access control, encryptie, audit logging en compliance met relevante standaarden. Test tegen de eisen van de eigen organisatie, zoals Baseline Informatie Beveiliging Overheid (BIO).
- Applicatiecompatibiliteit: Voer PoCs uit met kritische applicaties (zoals databases, ERP-systemen, legacy-applicaties) om te valideren of deze stabiel en performant draaien op het nieuwe platform.
- Migratie en interoperabiliteit: Simuleer de migratie van bestaande virtuele machines naar het nieuwe platform en test de interoperabiliteit met andere systemen (zoals storage, netwerk, cloud-integraties).
- Gebruikerservaring en beheer: Laat beheerders en eindgebruikers werken met het nieuwe platform om gebruiksvriendelijkheid, selfservice-mogelijkheden en support te beoordelen.

2.3.5 Aanbesteding(en) en roadmap

Aanbesteding(en)

Overheidsorganisaties hebben te maken met wetgeving rondom aanbesteding. Omdat de contracten rondom (beheer van) software vaak om grote bedragen gaat, is het aannemelijk dat voor de meeste software om een (virtualisatie)platform te realiseren een aanbesteding nodig is. Het kan zelfs zijn dat meerdere aanbestedingen nodig zijn als het platform opgedeeld wordt in meerdere stukken (bijvoorbeeld aparte virtualisatie- en containerplatformen, of wanneer gekozen is om meerdere leveranciers naast elkaar te gebruiken) en/of bepaalde functies (bijvoorbeeld beveiligingssoftware) apart ingekocht worden, omdat die geen directe afhankelijkheid hebben op het onderliggende platform.

Als besloten wordt om geheel over te gaan op open source zonder licenties, en beheer en onderhoud binnen de eigen organisatie of in samenwerking met meerdere organisaties gedaan wordt, kan het zijn dat een aanbesteding niet nodig is. Dit heeft echter grote organisatorische consequenties, omdat de organisatie dan alle expertise in de eigen gelederen moet hebben of moet kunnen halen bij een andere overheidsorganisatie. In het laatste geval wordt dus verdergegaan dan alleen centrale inkoop en dient er een overheidsorganisatie te zijn die de nodig expertise levert.

Als er sprake is van een aanbesteding, kunnen sommige onderdelen van de Proof of Concept fase mogelijk onderdeel zijn van de aanbesteding. Leveranciers wordt dan gevraagd om aan te tonen dat zij de betreffende functionaliteit kunnen leveren conform de opgestelde eisen en op een manier waarop de afnemer kan bepalen welke leverancier de beste oplossing heeft.

Roadmap en projectplan opstellen

Na de aanbesteding en de daarbij behorende definitieve selectie van een platform, dient een roadmap en projectplan opgesteld te worden. Aangezien bij de meeste organisaties het IT-landschap complex is en een migratie een aanzienlijke hoeveelheid applicaties bevat, is een gefaseerde migratie, eventueel met parallelle uitrol tijdens de testfase van een applicatie aan te bevelen. Voordat dit echter kan beginnen zal op z'n minst een basis-uitrol van het nieuwe platform plaats moeten vinden, zodat alle platform functies goed getest kunnen worden. Bij voorkeur wordt het platform na die uitrol uitgebreid, naarmate meer applicaties op het platform landen. Daarvoor is het dus nodig dat het platform eenvoudig uitgebreid kan worden.

Wanneer hardware uit het bronplatform nog niet aan het einde van de levenscyclus is en deze compatibel (verenigbaar) is met het nieuwe platform, heeft het uiteraard de voorkeur dat hardware hergebruikt kan worden.

Op basis van de inventarisatie van de applicaties kunnen clusters van applicaties geïdentificeerd worden die gezamenlijk gemigreerd kunnen of moeten worden. Daarbij is het aan te bevelen het migratieproject voor een cluster op te delen in logische fases, zoals voorbereiding, pilot, uitrol, optimalisatie en nazorg. De hardware die vrijgekomen is uit het bronplatform kan na elke fase mogelijk hergebruikt worden voor de volgende cluster aan applicaties. Voor iedere cluster is het van belang om eerst een risicoanalyse uit te voeren. Breng potentiële risico's in kaart, zoals downtime, dataverlies, compliance-issues en kennisverlies. Op basis daarvan kunnen mitigerende maatregelen uitgewerkt worden zoals fallback-scenario's, extra support en monitoring tijdens kritieke fases. Aan het eind van de migratie van iedere cluster, dienen de lessen die daaruit getrokken zijn gedocumenteerd te worden en meegenomen te worden naar de migratie van de volgende cluster. Dit biedt mogelijk ook kansen om bepaalde processen te automatiseren, zodat deze minder foutgevoelig zijn bij de volgende migratiecluster.

Tijdens de migratie is communicatie en verandermanagement een belangrijke component voor succes. Stel een communicatieplan op aan de hand waarvan alle stakeholders tijdig en transparant geïnformeerd worden over de voortgang, impact en verwachtingen. Zorg voor draagvlak en formele goedkeuring waar nodig.

Pilot en implementatieproces

De pilotfase bestaat uit twee stappen. De eerste stap is de initiële uitrol van het platform, zodat alle kernfunctionaliteit getest kunnen worden. Dit vormt de basis voor verdere uitbreiding. Het gaat hierbij niet alleen om het testen van de techniek, maar ook van de governance en de operatie van de verschillende teams die een rol spelen bij het opereren van het platform en het uitrollen van applicaties daarop. In de tweede stap wordt een beperkt aantal applicaties, bij voorkeur met verschillende eisen, uitgerold op het platform, zodat duidelijk wordt of de techniek zich zo gedraagt als bedoeld en of de processen conform verwachting verlopen. Voor elk van de applicaties dienen mitigerende maatregelen uitgewerkt te worden voor risico's die kunnen optreden, zoals dataverlies of ongewenste downtime.

Onderdeel daarvan is een terugrol scenario, zodat bij problemen teruggevallen kan worden op de oude situatie. Daar waar mogelijk zou gebruik gemaakt kunnen worden van parallel operatie, zodat getest kan worden of het nieuwe systeem precies zo reageert als het oude.

Het is belangrijk dat alle bevindingen en leerpunten goed gedocumenteerd worden, zodat in de verdere implementatiefase dezelfde problemen niet nogmaals optreden en/of men weet hoe problemen op te lossen. Ook in het verder proces is dit van belang, want daarmee kunnen standaardprocedures uitgewerkt worden in geval van problemen.

Na de pilot kan het platform stapsgewijs uitgebreid worden, waarin telkens clusters van applicaties gemigreerd worden. Automatisering van het migratieproces helpt daarbij om fouten te minimaliseren. Indien hardware hergebruikt kan worden, kan na het migreren van een cluster van applicaties de ouder omgeving geoptimaliseerd worden, zodat hardware vrijgemaakt kan worden en overgezet kan worden naar het nieuwe platform. Na elke clustermigratie kan een optimalisatieslag uitgevoerd worden en dient continuïteit en compliance geborgd te worden. Eventuele nieuwe problemen en de oplossingen daarvan dienen zoals eerder gezegd opgenomen te worden in standaardprocedures.

Tijdens alle fases is het cruciaal om governance, observability en integratie met bestaande beheersystemen te waarborgen. Dit zorgt voor controle, veiligheid en schaalbaarheid.

Hoofdstuk 3 - Besliscriteria

Besliscriteria zijn objectieve criteria waartegen verschillende oplossingen getoetst kunnen worden en op basis waarvan een selectie gemaakt kan worden. Voor elk criterium kan een score toegekend worden aan de oplossing. De weging van de verschillende score hangt af van de strategische doelstellingen die aan het begin van het selectieproces zijn vastgesteld. De besliscriteria besproken in dit hoofdstuk zijn op enkele criteria na generiek toe te passen op een selectieproces. De elementen waarmee bepaald wordt in hoeverre een oplossing aan een criterium voldoet kunnen meer specifiek zijn aan een virtualisatieplatform. In Appendix C – Virtualisatieplatformen zijn meerdere oplossingen getoetst aan de hand van de in dit hoofdstuk beschreven besliscriteria.

3.1 Overzicht van de besliscriteria

De onderstaande tabel laat zien welke onderdelen daarbij opgenomen worden. De gearceerde criteria zijn daarbij specifiek voor een virtualisatieplatform. De overige criteria kunnen, met enige aanpassing, ook toegepast worden op selectie van andere software.

Criterium	Omschrijving
Kernfuncties en kenmerken van het platform	
Virtualisatie/hypervisor	De kern van het virtualisatieplatform.
Opslag en opslagintegratie	De mogelijkheden voor het leveren van opslag (disks) aan het virtualisatieplatform.
(Software Defined) Netwerken	De manier waarop het netwerk geleverd wordt en samenwerkt met het virtualisatieplatform.
Bedrijfscontinuïteit	De mogelijkheden om applicaties actief te houden of snel weer actief te maken bij problemen of rampen.
Beveiliging en compliance	De functies die het platform biedt om gebruikers te autoriseren voor specifieke functies en te monitoren wat er gebeurt in het platform.
Beheer en automatisering	
Ondersteuning en beheer van containers	De functies die het platform biedt om te werken met containers conform de CNCF standaard.
Lifecycle management	De manier waarop patches en nieuwe versies uitgerold kunnen worden met minimale verstoring.
Automatisering en orkestratie	De mogelijkheden tot automatisering en orkestratie zodat systemen eenvoudig uitgerold en aangepast kunnen worden.
Observability en monitoring	De beschikbare functies om de omgeving en applicaties daarbinnen de monitoren.
Integratie met bestaande tooling	Integratie met 3rd party systemen voor netwerkbeheer, monitoring, asset management, beveiliging etc.

Bedrijfsvoering, operationele factoren en kosten	
Impact op de organisatie	Veranderingen die nodig zijn aan de organisatie bij adoptie van de betreffende oplossing.
Licentie en abonnement	Hoe de kosten voor softwarelicenties en onderhoudscontracten berekend worden.
Overdraagbaarheid van licenties	Of licenties overdraagbaar zijn naar andere infrastructuur.
Ondersteuningsmodel en ecosysteem	Hoe de leverancier haar klanten ondersteunt en hoe het ecosysteem om de oplossing heen daarin kan bijdragen.
Migratie en exit	De inspanning die vereist is voor de migratie en welke tooling daarvoor beschikbaar is.
Innovatie	De mate waarin de leverancier investeert in de innovatie van de oplossing.
Omscholing en beschikbaarheid van talent	De mogelijkheden die er zijn om medewerkers om te scholen en of er voldoende talent in de markt is om tijdelijk of permanent benodigde expertise te leveren.
Autonomie en continuïteit van de leverancier	In hoeverre een buitenlandse mogendheid kan beïnvloeden of de leverancier diensten kan blijven leveren.
Kosten (Total Cost of Ownership)	De manier waarop de kosten van de gehele oplossing berekend worden.

Figuur 9: Overzicht van besliscriteria

3.2 Besliscriteria

3.2.1 Kernfuncties en kenmerken van het platform

Virtualisatie/hypervisor

De kernfunctionaliteit die geleverd dient te worden is die van de virtualisatie/hypervisor die het mogelijk maakt om de onderliggende hardware op te delen in meerdere virtuele machines die op verschillende manieren samen kunnen werken via een (virtueel) netwerk.

De aspecten die belangrijk zijn bij evaluatie van de hypervisor zijn:

- Stabiliteit
- Efficiency
- Schaalbaarheid
- Compatibiliteit met specifieke hardware en aanpalende infrastructuur (bijvoorbeeld specifieke connectiviteit naar opslagsystemen, netwerkkaarten, -protocollen).
- Compatibiliteit met gast operating systemen
- Compatibiliteit met specifieke software

De eerste twee zijn relevant voor alle organisaties, terwijl de laatste vier meer organisatiespecifiek zijn. Dit omdat sommige organisaties voornamelijk werken met standaard hardware en software en weinig verandering ervaren in gebruik, terwijl andere juist specifieke toepassingen hebben of flexibel capaciteit moeten kunnen uitbreiden.

Opslag en opslagintegratie

Voor de disks van de virtuele machines is opslag nodig en deze dient geïntegreerd te zijn met het virtualisatieplatform om dit naadloos aan te kunnen bieden, buiten de eerder al genoemde hardware compatibiliteit. Voor de opslag is enerzijds van belang welke mogelijkheden het biedt voor diverse soorten opslag en anderzijds hoe het integreert met de virtualisatieoplossing.

De aspecten die belangrijk zijn bij evaluatie van de opslag:

- De betrouwbaarheid van het opslagsysteem, waarbij een aanpak gebruikt wordt om hoog beschikbare opslag te leveren met KPIs. Hierbij kan gedacht worden aan mogelijkheden als het gebruik van disk arrays, dual controller en multi-path ondersteuning.
- Welke ondersteuning het opslagsysteem biedt voor verschillende uitrolmodellen, te weten gecombineerde rekenkracht en opslag (binnen een Hyper Converged Infrastructure), gecentraliseerde opslag en speciale topologie met datareplicatie over meerdere locaties (zie ook 3.2.1.4 Bedrijfscontinuïteit).
- De manier(en) waarop de opslag integreert met de virtualisatieoplossing, waaronder de ondersteunde protocollen (bijvoorbeeld NFS, iSCSI, SMB, Fiber Channel), eventueel inclusief eventuele certificering voor deze protocollen.
- Mogelijkheden voor het veiligstellen van data (bijvoorbeeld snapshots).
- Mogelijkheden voor het beveiligen van data (bijvoorbeeld encryptie in opslag en transport, wissen van disks).
- Mogelijkheden voor optimalisatie van opslagverbruik en snelheid van lees- en schrijfoperaties, en het combineren van HDD, SSD en NVMe, hetgeen (deels) invloed kunnen hebben op de Total Cost of Ownership.

(Software Defined) Netwerken

Het virtualisatieplatform moet integreren in het netwerk, zodat applicaties ontsloten kunnen worden. Daarbij zijn er grofweg twee mogelijkheden:

1. Het virtualisatieplatform wordt aangesloten op een netwerk, waarbij het virtualisatieplatform verder verantwoordelijk is voor de indeling van het netwerk binnen de gevirtualiseerde infrastructuur. Beheer van het verder netwerk ligt buiten het virtualisatieplatform.
2. Het virtualisatieplatform integreert met een software-defined netwerk. Hierbij werken het netwerk en het platform samen bij de netwerkconfiguratie, waardoor het platform niet een eigen intern netwerk beheert, maar er één integraal netwerk ontstaat waarin alle resources zijn aangesloten. Deze opzet wordt meestal toegepast wanneer functies zoals multi-tenancy, self-service, microsegmentatie en netwerkencryptie belangrijk zijn.

Voor kleine organisaties met een centrale IT-beheer functie is de eerste optie vaak voldoende, terwijl grotere organisaties met een meer gedistribueerd operatie model de tweede optie kunnen gebruiken.

Hoe het netwerk en het virtualisatieplatform georganiseerd zijn bepaalt welke eisen van belang zijn bij het zoeken naar een alternatief. In het eerste geval is mogelijk alleen van belang hoe het virtualisatieplatform aangesloten wordt op een netwerk. In het tweede geval is van belang hoe het netwerk en het virtualisatieplatform kunnen integreren. In het geval dat software die onder deel is van het virtualisatie platform gebruikt wordt voor het software defined netwerk, dan is het mogelijk ook nodig dat dit vervangen wordt.

De aspecten die belangrijk zijn bij evaluatie van de netwerkfunctie:

- De stabiliteit van het netwerk.
- Ondersteuning voor hybride netwerken, integratie met overige netwerken.
- Schaalbaarheid
- Automatisering via APIs.
- Infrastructuur georiënteerde en/of applicatie georiënteerde netwerkconcepten (bijvoorbeeld NSX Software Defined Network tegenover Kubernetes networking).

Bedrijfscontinuïteit

Bedrijfscontinuïteit betreft twee verschillende functies:

- Hoge) beschikbaarheid (of high-availability) van systemen, zodat ook wanneer er fouten optreden systemen actief blijven.
- Herstellen van een “ramp”, waarbij een ramp kan variëren van een menselijke fout, kwaadwillende acties, tot (natuur)rampen die zaken als stroomuitval veroorzaken, ook bekend als disaster recovery.

Noot: geopolitieke invloeden worden besproken in 3.2.3.8 Autonomie en continuïteit van de leverancier.

Voor beschikbaarheid is van belang hoe snel een systeem kan reageren op een probleem, zodat applicaties (schijnbaar) constant beschikbaar zijn en hoe moeilijk het is om dit te configureren en automatiseren.

Voor herstellen is van belang hoe snel een systeem weer beschikbaar is (Recovery Time Objective of RTO) en hoeveel data daarbij verloren is gegaan (Recovery Point Objective of RPO). Ook hier is van belang hoe eenvoudig dit te configureren en automatiseren is.

De definitie van criteria voor bedrijfscontinuïteit dienen op meerdere niveaus vastgesteld te worden: op de infrastructuur, het virtualisatieplatform en per applicatie of virtuele machine.

De aspecten die belangrijk zijn bij evaluatie van de bedrijfscontinuïteit:

- De hoeveelheid dataverlies.
- De tijd die nodig is om over te schakelen naar een ander systeem.
- Hoe gemakkelijk het is om de beschikbaarheidsfuncties te configureren.

Beveiliging en compliance

Beveiliging en compliance betreffen platform functies die integraal onderdeel van het platform om het systeem veilig te houden. Dit gaat daarmee om de beveiliging van de beheerfunctionaliteit (control plane), niet de beveiliging van applicaties en de daarmee samenhangende functies (data plane). Tools die additionele beveiliging bieden als bijvoorbeeld malware beveiliging vallen hier niet onder. Het gaat met name om welke functies geboden worden om toegang te beperken, ongeautoriseerde toegang te detecteren, en aan te kunnen tonen dat aan specifieke standaarden voldaan wordt.

De aspecten die belangrijk zijn bij evaluatie van de beveiliging en compliance:

- Ondersteuning voor Multi-Factor Authentication (MFA).
- Ondersteuning voor Role Based Access Control (RBAC).
- Ondersteuning van encryptie voor dataopslag en transport.
- De beschikbaarheid over audit logs.
- De mogelijkheden voor monitoring.

3.2.2 Beheer en automatisering

Ondersteuning en beheer van containers

Moderniseren van het applicatielandschap staat in principe los van de keuze voor een (nieuw) virtualisatieplatform. Modernisering biedt echter naast betere functionaliteit voor gebruikers ook de mogelijkheid om applicaties minder afhankelijk te maken van de onderliggende infrastructuur door gebruik te maken van containers. Dit is daarom een belangrijk onderdeel om flexibeler te worden en niet meer van een specifieke leverancier afhankelijk te zijn voor virtualisatie. Door applicaties zogenaamd “cloud native” te maken, kunnen applicaties uitgevoerd worden in containers die op willekeurige (virtuele) servers kunnen werken.

De *de facto* standaard voor container beheer en orkestratie is Kubernetes, open source software wordt ontwikkeld en onderhouden door Cloud Native Compute Foundation (CNCF). Applicaties die conform de CNCF standaard ontwikkeld worden kunnen in principe uitgevoerd worden op een willekeurige CNCF compliant omgeving.

Veel organisaties zijn al bezig met het moderniseren van applicaties en zoals eerder in het rapport aangegeven is het moderniseren van applicaties een manier om wendbaarder te worden. Wanneer gemoderniseerde applicaties moeten samenwerken met applicaties die nog in virtuele machines draaien, is het voordelig om een Kubernetes-implementatie te hebben die onderdeel vormt van, of goed integreert met, het virtualisatieplatform.

Belangrijke criteria voor de ondersteuning van containers zijn:

- Naleving van de CNCF standaard
- Schaalbaarheid
- Gebruiksgemak
- Integratie met de onderliggende infrastructuur en hybride mogelijkheden

Lifecycle management

Lifecycle management betreft het bijwerken van de software van het platform met minimale verstoring. Hierbij is van belang dat er consistente en automatische uitrol plaatsvindt van de platform software, eventuele add-ons van de hardware leverancier en firmware en drivers, en dat dit gefaseerd gaat om te zorgen niet het hele platform in één keer helemaal onbeschikbaar is. Sommige platformen bieden hierbij eventueel de mogelijkheid om virtuele machines te verplaatsen naar een andere fysieke server terwijl ze actief blijven (live migration), zodat een fysieke server pas bijgewerkt wordt als er geen actieve applicaties op draaien.

Belangrijke criteria voor lifecycle management zijn:

- Het correct uitvoeren van alle nodige updates met minimale verstoring.
- De efficiency van updates en beheeractiviteiten.
- Integratie met bestaande tools zoals

bijvoorbeeld command-line en scripting interfaces, configuration management bijvoorbeeld Ansible, Puppet), Infrastructure-as-Code (bijvoorbeeld Terraform).

Automatisering en orkestratie

Automatisering en orkestratie betreft het eenvoudig uit kunnen rollen en aanpassen van systemen. Enerzijds vanuit het perspectief van autonomie van gebruikers om binnen vastgestelde kaders (bijvoorbeeld het aantal virtuele processoren of specifieke beveiligingsmaatregelen) zonder tussenkomst van een beheerder taken uit te kunnen voeren, anderzijds vanuit het perspectief van procesautomatisering.

Belangrijke criteria voor automatisering en orkestratie zijn:

- Mate van mogelijke automatisering.
- Integratie met bestaande tools zoals bijvoorbeeld command-line en scripting interfaces, configuration management (bijvoorbeeld Ansible), Infrastructure-as-Code (bijvoorbeeld Terraform).
- Schaalbaarheid.
- Efficiëntie en gebruiksvriendelijkheid.
- Mogelijkheid om compliance af te dwingen met technische kaderstelling.
- Functionaliteit van een gebruikersportaal.

Observability en monitoring

Observability en monitoring betreft het inzicht aangaande wat er in het systeem gebeurt om fouten op te kunnen lossen en om capaciteit te plannen. Het platform moet voldoende informatie leveren om te kunnen zien wat de status van het systeem is, hoeveel capaciteit beschikbaar is, en waardoor bepaalde fouten ontstaan. Waar mogelijk dient het platform ook mogelijkheden te bieden om fouten op te lossen. Over het algemeen geldt dat hoe transparanter het platform, hoe beter.

Belangrijke criteria voor automatisering en orkestratie zijn:

- De mogelijke meetpunten waarvoor data inzichtelijk gemaakt kan worden.
- Hoe makkelijk het is om inzicht te krijgen in dat wat belangrijk is.
- Hoe snel de meetdata beschikbaar is (bijvoorbeeld real-time).

Integratie in bestaande (3rd party) beheersystemen

Veel organisaties gebruiken 3rd party tools voor zaken als asset management, monitoring/observability, netwerken en beveiliging. Vaak gebruikte tools hiervoor betreffen:

- **Cisco ACI (Application Centric Infrastructure)** – Software Defined Networking
- **Flexera** – IT Asset Management
- **New Relic** – Monitoring en observability om door hele technologie stack inzichten te krijgen
- **Qualys VMDR** – Vulnerability management
- **Rubrik** – Data security
- **Splunk** – Logaggregatie en analyse voor met name beveiliging

Aangezien verschillende organisaties verschillende tools kunnen gebruiken, is het niet mogelijk om een uitputtende lijst te maken met alle tools waarmee geïntegreerd moet worden. In hoeverre oplossingen integraties met de bovenstaande tools leveren, kan een indicatie geven of een oplossing open of gesloten is als het gaat om integraties met 3rd party tools. Iedere organisatie zal bij het selectieproces moeten nagaan welke tools mee geïntegreerd moet worden en onderzoek moeten doen in hoeverre aan de criteria voldaan wordt.

Belangrijke criteria voor integratie zijn:

- Compatibiliteit
- Hoe ver de integratie reikt.
- De beschikbaarheid van plug-ins voor integratie.
- De beschikbaarheid van gezamenlijke functionaliteit en ondersteuning.

3.2.3 Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

De adoptie van een ander platform vergt niet alleen aanpassingen op technisch vlak. Zelfs als alleen gekozen wordt voor een ander virtualisatieplatform, heeft dit impact op de kennis en kunde die de organisatie moet hebben en is een verandertraject en omscholing vereist.

Wanneer gekozen wordt voor het vervangen van het bestaande virtualisatieplatform, kan ook gekozen worden voor een verdergaande verandering in hoe applicaties ontwikkeld en uitgevoerd worden, door in te zetten op het moderniseren van applicaties middels containertechnologie.

Hierbij kan ook gekeken worden naar het vervangen van eigen ontwikkelde applicaties naar standaardsoftware die gebruik maakt van een moderne architectuur. Hoewel deze route meer technologische verandering en daarmee mogelijk meer veranderkosten met zich meebrengt, biedt deze optie op de langere termijn meer flexibiliteit, waardoor het eenvoudiger wordt om van leverancier te wisselen als de leverancier van strategie verandert of failliet gaat.

Dergelijke modernisatie heeft invloed op welke rollen binnen de organisatie nodig zijn en vraagt om uitgebreid verandermanagement. Afhankelijk van de snelheid en en hoe ingrijpend de wijzigingen in de organisatie zijn, kan goedkeuring van de Ondernemingsraad (OR) vereist zijn.

Aangezien het moderniseren van applicaties behoorlijke inspanning vergt, kan het daarnaast nodig zijn om voor een aantal jaar een tweesporenbeleid te voeren, waarbij een deel van de applicaties gevirtualiseerd blijft, terwijl andere applicaties aangepast worden. Hierbij kan (ook) naar een nieuw virtualisatieplatform gemigreerd worden of gekeken worden naar het optimaliseren van het huidige platform voor de duur van het modernisatietraject.

Als gekozen wordt voor modernisatie, zal het beheer van de fysieke infrastructuur niet significant wijzigen. Platformbeheer, netwerkbeheer, architectuur, applicatieontwikkeling en -beheer veranderen echter wel significant. In een gemoderniseerd landschap worden applicaties ontwikkeld en beheerd door DevOps teams die een hoge mate van autonomie hebben binnen vastgestelde kaders. Dit betekent dat in een modern landschap de volgende functies bestaan:

- Architectuur – Vastleggen van de kaders waarbinnen applicaties uitgevoerd moeten worden en definitie van zogenaamde Landing Zones.
- Infrastructuurbeheer – Beheer van de fysieke infrastructuur.
- Platformbeheer – Beheer van het virtualisatie en containerplatform, monitoring, en het verzorgen van de automatisering die ontwikkelteams in staat stelt om applicaties te ontwikkelen conform de vastgelegde kaders in Landing Zones.
- DevOps – Het ontwikkelen en opereren van applicaties binnen de vastgestelde Landing Zones, waarbij met behulp van Infrastructure-as-Code de juiste containerconfiguratie neergezet wordt waarop de applicatie uitgevoerd kan worden.

Belangrijke criteria voor het vaststellen van de impact op de organisatie zijn:

- De mate waarin rollen veranderen. Veranderen deze alleen qua technologie of ook qua rolverdeling?
- De impact op de grootte (aantal FTE) van bepaalde functies/teams binnen de organisatie.
- De mate waarin door rolverandering de organisatie aangepast dient te worden.
- Of Ondernemingsraad betrokken moet worden bij de verandering.

Licentie en abonnement

De aanleiding van dit rapport zijn de wijzigingen in de licentiestructuur en -kosten van VMware. Afhankelijk van hoe software gebruikt wordt, kunnen dergelijke wijzigingen in structuur en kosten bijdragen aan een aanzienlijk hogere prijs voor alle benodigde licenties en daarmee een hogere Total Cost of Ownership (TCO).

Bij een flexibele licentiestructuur kan de afnemer precies de licenties kiezen die het nodig heeft. Bij een minder flexibele structuur worden verschillende componenten gebundeld, waarbij de afnemer niet per definitie alle componenten gebruikt en dus meer betaalt voor een licentie dan nodig voor de gebruikte functionaliteit. Leveranciers bundelen licenties in de hoop dat afnemers ook de functionaliteit die niet nodig is gaan gebruiken om zo een hogere binding met de leverancier te creëren.

Bij open source is in principe geen sprake van licentiekosten, al kunnen open source componenten gebundeld zijn met close source componenten waarvoor licenties nodig zijn. Voor geheel open source pakketten zijn de kosten gerelateerd aan zekerheid dat de geleverde software aan bepaalde kwaliteitsstandaarden voldoen en aan de ondersteuning die geboden wordt wanneer er een probleem is. Er is derhalve meer sprake van een onderhoudsabonnement. Bij pure open source zijn deze kosten strikt genomen optioneel, maar zonder een dergelijke ondersteuning valt het valideren van de open sourcecomponenten en het oplossen van problemen volledig op de afnemer, die daarvoor vaak de kennis en kunde niet heeft.

Bij de meest gebruikelijke vorm van open source ondersteuning stelt de ondersteuner een zogenaamde distributie samen waarop ondersteuning gegeven wordt. Er wordt dus alleen op een hele specifieke versie ondersteuning geleverd. Wil een organisatie naar een andere partij overstappen, dan moet de distributie van die andere partij gebruikt worden, waardoor alle systemen opnieuw ingericht moeten worden.

De kosten van een licentie of abonnement worden berekend per een afname eenheid, bijvoorbeeld per CPU, per core, per gebruiker, of per hoeveelheid opslag.

Belangrijke criteria voor licentie en abonnement zijn:

- Flexibiliteit van de licentie: is het mogelijk een licentie af te nemen voor alleen die componenten die gebruikt worden?
- Het prijsmodel: is er sprake van een eenmalige betaling voor een licentie van een specifieke versie (capex) of is er sprake van een abonnement waarin nieuwe versies meegenomen zijn en die voor een bepaalde tijd afgesloten wordt (opex, pay-per-use)?
- Stabiliteit van de prijs/kosten: in hoeverre kan de prijs van licenties tijdens de contractduur veranderen en welke prijsstijgingen zijn te verwachten bij het afsluiten van een nieuw contract?
- De kosten van de licentie of het abonnement en de afname eenheid.
- De complexiteit en transparantie van de licentie of abonnement.

Overdraagbaarheid van licenties

Als een licentie overdraagbaar is, kan deze meegenomen worden naar een andere omgeving. Dat kan zijn als nieuwe hardware aangeschaft wordt om oude te vervangen en als van on-premises naar cloud of naar een hosting partij verhuisd wordt.

Belangrijke criteria voor overdraagbaarheid van licenties zijn:

- Is overdracht mogelijk van de ene infrastructuur naar de andere?
- Is overdracht mogelijk naar een cloud platform?
- Zijn er kosten verbonden aan de overdracht?

Ondersteuningsmodel en ecosysteem

Voor vrijwel alle organisaties geldt dat niet alle benodigde kennis en kunde voor het opereren van het virtualisatieplatform intern georganiseerd kan worden, aangezien dit zeer specialistische kennis vereist die maar sporadisch nodig is. De benodigde kennis kan bij de leverancier vandaan komen, maar ook uit andere organisaties of uit een ecosysteem van (kleine) bedrijven en freelancers.

Belangrijke criteria voor ondersteuningsmodel en ecosysteem zijn

- Hoe biedt de leverancier ondersteuning?
- Hoe is de lange termijn ondersteuning (o.a. updates, patches) geregeld?
- Biedt de leverancier extra diensten, zoals advies en technisch accountmanagement?
- Wat is de kwaliteit van het partner ecosysteem?
- Wat is de kwaliteit van het verdere ecosysteem (o.a. freelancers, contributors aan open source)?

Migratie en exit

Indien gemigreerd moet worden van een platform naar een ander, hangt de impact van de migratie af van de beschikbare tooling en de mate van verstoring van lopende systemen. Bij voorkeur kan een systeem gemigreerd worden zonder dat dit verstoring oplevert (live migration), maar als dit niet mogelijk is, dient de verstoring geminimaliseerd te worden.

De tooling die gebruikt kan worden voor migratie, zou ook van toepassing moeten zijn op een exit, wat gezien kan worden als een omgekeerde migratie.

Belangrijke criteria voor ondersteuningsmodel en ecosysteem zijn:

- Compatibiliteit met het bronplatform en het doelplatform.
- Complexiteit (mate van handmatige en automatische acties).
- Ondersteuning door tools.

Innovatie

Het platform dient mee te kunnen ontwikkelen met de veranderende behoeften van organisaties en in te spelen op ontwikkelingen in de markt. Bij de evaluatie van platformen dient daarom gekeken te worden naar hoe de leverancier omgaat met ontwikkeling van nieuwe mogelijkheden die hiervoor zorgen.

Belangrijke criteria voor innovatie zijn:

- In hoeverre is het platform markt leidend of niche?
- (Hoe) wordt er geïnvesteerd in de evolutie van het platform?
- Hoe vaak worden functie-uitbreidingen (feature updates) uitgebracht?
- Hoe is AI onderdeel van de product evolutie?
- Met welke partners wordt samengewerkt op het gebied van innovatie?

Omscholing en beschikbaarheid van talent

Het adopteren van een ander platform gaat gepaard met het opbouwen van de benodigde kennis en kunde. Voor een organisatie is enerzijds belangrijk welke mogelijkheden er zijn om bestaand personeel op te leiden en anderzijds wat de beschikbaarheid is van professionals in de markt.

Hierbij kan gekeken worden naar tijdelijke inhuur van professionals om tijdelijk het bestaande team te helpen met de opbouw van het platform en de daarbij benodigde kennis en kunde. Echter, aangezien het voor kan komen dat sommige mensen binnen het bestaande personeelsbestand niet in staat zijn om voldoende dan wel snel genoeg kennis op te bouwen, kan het nodig zijn om permanent nieuwe mensen aan te trekken. Daarmee kan het nodig zijn om actief personeelsbeleid te voeren rondom de adoptie van een nieuw platform. Zoals besproken in 3.2.3.1 Impact op de organisatie goedkeuring van de ondernemingsraad (OR) nodig zijn als dit leidt tot significante organisatiewijzigingen.

Belangrijke criteria voor omscholing en beschikbaarheid van talent zijn:

- Benodigde tijd en kosten om de nodige kennis en kunde op te bouwen.
- Beschikbaarheid van professionals in de markt, zowel bij grotere organisaties als zelfstandigen.
- Beschikbare trainingen en certificeringen.
- Beschikbaarheid van goede documentatie.
- Grootte van de community rondom het platform, zodat vragen gesteld kunnen worden op online fora.

Autonomie en continuïteit van de leverancier

Vanwege geopolitieke en economische krachten dient meegewogen te worden in hoeverre een oplossing onder invloed kan vallen van overheden en/of marktpartijen (buiten de EU) en of deze partijen de levering van software en beheer kunnen blokkeren (ook wel een “kill switch” genoemd).

Hierbij zijn een aantal zaken van belang:

- Closed source versus open source.
- Het aantal en de herkomst van ontwikkelaars die de software ontwikkelen en onderhouden.
- De herkomst van de organisatie(s) die de oplossing ontwikkelt en onderhoudt en indien de organisatie gevestigd is in de EU hoe deze beschermt is tegen overname door een organisatie buiten de EU.
- Het aantal organisaties dat betrokken is bij het ontwikkelen en onderhouden van de software (met name bij open source).
- Het type organisatie(s) dat de software ontwikkelt en onderhoudt (commercieel, non-profit, overheid).
- De manier waarop kwaliteit en continuïteit geborgd worden.
- De impact wanneer de oplossing niet meer geleverd kan worden door de organisatie die de oplossing ontwikkelt en onderhoudt.
- De mate waarin aangeschafte hardware ook met andere oplossingen te gebruiken is.

Kosten (Total Cost of Ownership)

Uiteindelijk is een van de sleutelonderdelen voor een keuze voor een specifiek platform de totale kosten voor de aanschaf en het beheer van het platform over een bepaalde periode. De tabel hieronder geeft een overzicht van de investeringen en operationele uitgaven voor verschillende factoren die deze kosten beïnvloeden, alsmede de kosten- en risicofactoren die daar invloed op kunnen hebben. Uitgaande van vergelijkbare efficiency van de hypervisor, zullen datacenter- en infrastructuurkosten voor alle oplossingen vergelijkbaar zijn, terwijl de andere factoren meer beïnvloed worden door de keuze van het virtualisatieplatform.

Factor	Investeringen (CapEx)	Operationele uitgaven (OpEx)	Kosten- en risicofactoren
Datacenter	Constructie of aankoop	Elektriciteit, koeling, facilitair beheer	Energiekosten, efficiëntie (PUE), ruimtebenutting
Infrastructuur	Aankoop van servers, opslagsystemen, netwerkapparatuur	Reparaties, onderhoudscontracten	Capaciteitsbehoefte, Hardware lifecycle, vendor lock-in, toeleveringsketen
Software (virtualisatie, beheer, backup, monitoring)	Initiële licentiekosten voor hypervirtualisatie-platform en beheertools	Terugkerende kosten voor licenties of onderhoudscontracten	Wijzigingen in licentiemodellen, versie-upgrades, vendor lock-in
Training & Certificering	Initiële trainingsprogramma's voor IT-personeel	Voortdurende training, certificeringsverlengingen	Hoge verloop, evoluerende technologiestack, vaardigheidstekorten
Migratiekosten	Tools voor migratie, tijdelijke hardware	Adviesdiensten, uitgebreide ondersteuning tijdens migratie	Datacomplexiteit, stilstandsrisico, projectoverlopen
Verandermanagement	Verandermanagementtools, communicatieplatforms	Programma's voor personeelsbetrokkenheid, procesherontwerp	Verzet tegen verandering, productiviteitsdalingen, culturele uitdagingen
Beheer	Opzetten beheerprocessen	Uitvoering beheerprocessen	Complexiteit van de hardware en software, wijzigingen aan hardware en software, mate van automatisering

Figuur 10: TCO factoren en risco's

Hoofdstuk 4 - Conclusies en aanbevelingen

4.1 Bouwen aan meer autonomie en weerbaarheid

Met de verandering en in de geopolitieke situatie is het zaak voor de overheid om niet alleen meer te kijken naar de beste kwaliteit tegen de laagste kosten, maar om ook mee te wegen hoe geopolitieke afhankelijkheid verminderd kan worden. Waar in rapport “Van kwetsbaar naar weerbaar” aanbevelingen gegeven worden richting de overheid als geheel, richt dit rapport zich op wat organisaties zelf kunnen doen.

Het opbouwen van meer autonomie en weerbaarheid vergt een lange adem. Een eigen infrastructuur bouwen zoals de Rijkscloud kan daarin een rol spelen in de komende jaren, maar autonomie en weerbaarheid gaat verder dan infrastructuur. Het vereist een grondige aanpassing in hoe systemen ontwikkeld of geselecteerd worden en hoe deze geopereerd worden. Dit is veel ingrijpender, omdat dit verandering vereist in expertise, architectuur en organisatie, en dit raakt in potentie vrijwel elk systeem binnen de overheid. Het is daarom ook belangrijk niet te veel tegelijk te willen doen. Denk groot, maar begin klein en breidt uit in kleine stapjes.

Het is aan te bevelen om bepaalde activiteiten meer te beschouwen als terugkerende activiteiten, om zo een beeld te hebben van waar de kansen en uitdagingen liggen. Zo is het van belang om risicoanalyse dynamisch te doen en bij grote wijzigingen in het risicobeeld dit voor te leggen aan het CIO-beraad, zodat daarover beleidsbesluiten genomen kunnen worden. Daarnaast is een goed gecategoriseerd IT-landschap hebben waarin duidelijk is hoe kritiek systemen zijn, om het verminderen van afhankelijkheden ingebed te hebben in architectuurontwikkeling, en om exit- en migratieplannen standaard onderdeel te maken van het ontwikkelproces van systemen. De overheid kan niet alles zelf en moet dat ook niet willen. Het is daarom naast het opbouwen van eigen expertise ook aan te bevelen om te denken in termen van het opbouwen van een ecosysteem. De overheid kan voorwaarden in de markt scheppen om oplossingen te ontwikkelen die de overheid vooruithelpen en interessant zijn voor marktpartijen om in te investeren.

Hierbij is het wel van belang dat overheidsorganisaties op grote lijnen dezelfde richting op bewegen en dit ook met elkaar coördineren. De aanbevelingen kunnen als volgt samengevat worden:

- Categoriseer applicaties aan de hand van (geopolitieke) risico’s die de continuïteit bedreigen en de impact daarvan op de organisatie.
- Definieer architectuur die de juiste oplossing (archetype) koppelt aan de mate van risico en impact, en volg een programmatische aanpak om autonomie en weerbaarheid te verbeteren. Werk samen met andere overheidsorganisaties om referentiearchitecturen (verder) uit te werken.
- Gebruik waar mogelijk open standaarden en de facto (open source) standaarden.
- Maak de organisatie beter geschikt om met open source te werken, aangezien dit een ander operationeel model vereist. Zoek hiervoor samenwerking met andere organisaties om de organisatorische impact te beperken.
- Bouw een ecosysteem binnen de overheid en met de markt waarmee meer autonomie mogelijk wordt.
- Versterk leveranciersmanagement met duidelijke (strategische) criteria opgezet te worden waaraan leveranciers getoetst kunnen worden en aan de hand waarvan contracten onderhandeld worden.
- Neem clausules op in contracten over de rechten die de organisatie heeft wanneer de leverancier overgenomen wordt. Dit kunnen clausules betreffen die beschermen tegen prijsverhogingen, wijzigingen in licentiestructuur en de mogelijkheid om zonder boete naar een andere leverancier over te stappen.

4.2 Verminderen leveranciersafhankelijkheid

Minder afhankelijk worden van leveranciers kan op verschillende manieren, waarbij een exit-plan of het gebruik van meerdere leveranciers een verandering betekent in de relatie tot leveranciers. Het gebruik van open source als derde optie betekent dat een ander type leverancier nodig is en/of de organisatie zelf meer kennis op moet bouwen van de interne werking van software, omdat veranderingen aan de software niet meer per definitie van de leverancier komen en daardoor goed gecontroleerd moeten worden. Dit leidt tot de volgende aanbevelingen:

- Maak exit-strategie/plan onderdeel van de leverancierselectie.

- Stel eisen aan leveranciers om een exit te faciliteren. Enerzijds door onder bepaalde voorwaarden een exit mogelijk te maken zonder contractuele boetes, anderzijds met technische ondersteuning om een exit mogelijk te maken.
- Overweeg meerdere leveranciers voor dezelfde functionaliteit wanneer het mogelijk is om de organisatie te segmenteren, zodat de mogelijkheid er is om tussen platformen te verplaatsen. Wees bewust dat dit organisatorische overhead met zich meebrengt.
- Overweeg de toepassing van open source boven commerciële software, maar wees bewust dat dit een ander operationeel model vergt met meer expertise die binnen de organisatie nodig is.

Let op dat bij de keuze voor opensource software je de afhankelijkheid kan verminderen maar niet volledig kan wegnemen. Veel opensource pakketten worden beheerd of worden gesponsord door commerciële organisaties die een niet gewenste invloed kunnen uitoefenen. De keuze voor opensource kan niet los staan van de andere aanbevelingen.

4.3 Keuze virtualisatieplatform

De keuze voor een virtualisatieplatform is met name een tactische activiteit, waarbij de strategie wordt meegenomen in de besliscriteria en de weging daarvan. Ondanks dat dit een meer tactische keuze betreft, is het virtualisatieplatform voor veel organisaties de hoeksteen van het IT-landschap, waardoor veranderingen daaraan behoorlijke impact kunnen hebben. De keuze van een (nieuw) virtualisatieplatform is daardoor niet alleen een techniekkeuze, het kan een strategische keuze zijn die ook wijzigingen in de organisatie vereisen. Het is daarom van belang om al lang voordat een eventueel platformkeuze gedaan moet worden de strategische richting bepaald is en het proces van selectie in gang gezet wordt.

De oplossingsstrategie wordt gestuurd door twee kernoverwegingen:

- Het soort oplossing: virtualisatieplatform, containerplatform, private cloud platform.
- Het commerciële model: leverancier eigen, open source gebaseerd, volledig open source.

Deze twee overwegingen bepalen in grote mate hoe leveranciersmanagement, ontwikkeling en operatie moeten werken en heeft daarmee grote invloed op of en hoe de organisatie aangepast moet worden qua operationeel model. Deze overwegingen bepalen daarmee welke oplossingen geprioriteerd moeten worden in het selectieproces. In 2.3.1 Oplossingsstrategie zijn de verschillende platformen die in Appendix C – Virtualisatieplatformen zijn beoordeeld tegen de vastgestelde besliscriteria afgezet tegen deze strategische overwegingen.

Een van de grootste technische pijnpunten is de integratie van het fysieke netwerk en software gedefinieerde netwerken (SDN). Wanneer het laatste sterk geïntegreerd is in het virtualisatieplatform, zoals bijvoorbeeld met VMware NSX of Nutanix Flow, is de impact op een migratie naar een ander platform veel groter. Modernisering van het applicatielandschap vermindert de afhankelijkheid op het virtualisatieplatform en daarmee op de SDN-componenten, maar er blijven voorlopig systemen die niet gemoderniseerd kunnen worden om technische of economische redenen.

De belangrijkste aanbevelingen uit dit rapport zijn:

- Begin vroegtijdig met het proces van de vernieuwing van hardware of software. De impact van een wijziging is relatief groot en implementatie vergt over het algemeen meer dan een jaar voor grote omgevingen. Begin daarom in de regel minimaal 2 jaar van tevoren met plannen.
- Betrek ook andere onderdelen van de organisatie (o.a. finance, HR) in de aansturing van het selectietraject, zodat er goede borging is bij wijzigingen die verder gaan dan techniek.
- Bouw bij de keuze voor een open source platform interne expertise op om dit platform te kunnen ondersteunen wanneer de ondersteuning uit het ecosysteem of onderhoudspartij niet afdoende dekkend is.
- Voer als onderdeel van het proces een applicatierationalisatie uit om te bepalen wat er moet gebeuren met applicaties en of deze minder afhankelijk van het onderliggende platform gemaakt kunnen worden en daarmee minder afhankelijk van de leverancier.

Wanneer eenmaal overgegaan wordt op het selectieproces, dienen de besliscriteria in dit document als leidraad die verder uitgebreid kan worden en waarvan de weging aangepast kan worden. Criteria die gekoppeld zijn aan de soorten systemen die een organisatie draait op het platform (bijvoorbeeld Oracle, SAP), dienen verder uitgewerkt te worden om te toetsen aan de specifieke eisen van de organisatie.

4.4 Volgordelijkheid van de aanbevelingen

De aanbevelingen kennen een volg ordelijkheid om er voor te zorgen dat de keuzes die er gemaakt gaan worden op de juiste manier worden verankerd in de organisatie. Tevens is ook gekeken naar de prioriteit. Waarbij het in control zijn van de risico's de basis vormt. Tevens erkennen wij ook dat niet alle aanbevelingen opportuun zijn voor iedere organisatie en in sommige gevallen kunnen leiden tot complexiteit die niet gewenst is. Dit is voornamelijk het geval bij kleinere organisaties.

Dit leidt tot de volgende aanbevolen volgordelijkheid..

1. **Risicomanagement**
   - 1.1. Categoriseer applicaties aan de hand van (geopolitieke) risico's die de continuïteit bedreigen en de impact daarvan op de organisatie.

2. **Oplossingsrichting**
   - 2.1. Definieer architectuur die de juiste oplossing (archetype) koppelt aan de mate van risico en impact, en volg een programmatische aanpak om autonomie en weerbaarheid te verbeteren. Werk samen met andere overheidsorganisaties om referentiearchitecturen (verder) uit te werken.
   - 2.2. Gebruik waar mogelijk open standaarden en de facto (open source) standaarden.
   - 2.3. Overweeg de toepassing van open source boven commerciële software, maar wees bewust dat dit een ander operationeel model vergt met meer expertise die binnen de organisatie nodig is.
   - 2.4. Begin vroegtijdig met het proces van de vernieuwing van hardware of software. De impact van een wijziging is relatief groot en implementatie vergt over het algemeen meer dan een jaar voor grote omgevingen. Begin daarom in de regel minimaal 2 jaar van tevoren met plannen.
   - 2.5. Voer als onderdeel van het proces een applicatierationalisatie uit om te bepalen wat er moet gebeuren met applicaties en of deze minder afhankelijk van het onderliggende platform gemaakt kunnen worden en daarmee minder afhankelijk van de leverancier.

3. **Leveranciersmanagement en organisatie**
   - 3.1. Maak de organisatie beter geschikt om met open source te werken, aangezien dit een ander operationeel model vereist. Zoek hiervoor samenwerking met andere organisaties om de organisatorische impact te beperken.
   - 3.2. Bouw bij de keuze voor een open source platform interne expertise op om dit platform te kunnen ondersteunen wanneer de ondersteuning uit het ecosysteem of onderhoudspartij niet afdoende dekkend is.
   - 3.3. Versterk leveranciersmanagement met duidelijke (strategische) criteria waaraan leveranciers getoetst kunnen worden en aan de hand waarvan contracten onderhandeld worden.
   - 3.4. Neem clausules op in contracten over de rechten die de organisatie heeft wanneer de leverancier overgenomen wordt. Dit kunnen clausules betreffen die beschermen tegen prijsverhogingen, wijzigingen in licentiestructuur en de mogelijkheid om zonder boete naar een andere leverancier over te stappen.
   - 3.5. Maak exit-strategie/plan onderdeel van de leverancierselectie.
   - 3.6. Stel eisen aan leveranciers om een exit te faciliteren. Enerzijds door onder bepaalde voorwaarden een exit mogelijk te maken zonder contractuele boetes, anderzijds met technische ondersteuning om een exit mogelijk te maken.
   - 3.7. Overweeg meerdere leveranciers voor dezelfde functionaliteit wanneer het mogelijk is om de organisatie te segmenteren, zodat de mogelijkheid er is om tussen platformen te verplaatsen. Wees bewust dat dit organisatorische overhead met zich meebrengt.
   - 3.8. Betrek ook andere onderdelen van de organisatie (o.a. finance, HR) in de aansturing van het selectietraject, zodat er goede borging is bij wijzigingen die verder gaan dan techniek.
   - 3.9. Bouw een ecosysteem binnen de overheid en met de markt waarmee meer autonomie mogelijk wordt.

Appendix A - Moties en kamervragen

- **Moties debat afhankelijkheid Amerikaanse techbedrijven (13-03-2025):**
  - Motie 26643-1315: Stoppen met migraties van overheids-ICT naar clouddiensten van Amerikaanse techgiganten
  - Motie 26643-1316: Aanbesteding voor een rijkscloud in volledig Nederlands beheer
  - Motie 26643-1317: DNS-keten van het.nl-internetdomein in Nederland
    - Kamerbrief stand van zaken motie over .nl domein (12-08-2025)
  - Motie 26643-1318: Risicoanalyse en Exit-strategie voor clouddiensten van Amerikaanse Techgiganten
  - Motie 26643-1319: In EU-verband pleiten voor versnelde investeringen in Cloudinitiatieven
  - Motie 26643-1320: Doelstelling hanteren dat de continuïteit van de Nederlandse overheid niet rechtstreeks afhankelijk is van partijen uit de VS
  - Motie 26643-1323: Europese bedrijven op één te zetten bij aanbestedingen van vitale ICT-diensten en voor de rijksoverheid en lokale overheden samen met het bedrijfsleven alternatieven te ontwikkelen voor de grote Amerikaanse techbedrijven.

- **Kamervragen over de groeiende afhankelijkheid van Amerikaanse techgiganten (23-05-2025)**
  - Beantwoording (19-09-2025)

- **Initiatiefnota Wolken aan de horizon (18-06-2024)**

- **Kamervragen overname Zivver en Solvinity**
  - Kathmann (18-09-2025)
  - Kathmann (13-11-2025)
  - Jansen (26-11-2025)
  - Beantwoording (17-12-2025)

- **Kamervragen overstap Belastingdienst naar Microsoft (07-10-2025)**
  - Beantwoording (01-12-2025)
  - Vervolg Kathmann, Dassen, El Boujdaini (10-12-2025)

- **Kamervragen afhankelijkheid van de financiële sector van Amerikaanse techgiganten (05-11-2025)**
  - Beantwoording (05-12-2025):

Appendix B- Licentievormen

Wat zijn perpetual licenties?

Hoewel VMware ook subscriptions aanbood, kozen de meeste organisaties door de jaren voor de aanschaf van perpetual licenties. Dit betekende dat ze eenmalig betaalden en daarmee een eeuwigdurend gebruiksrecht kregen voor afgesproken softwareversies waarbij betaald werd voor jaarlijkse maintenance (software updates, patches en bugfixes) en support (technische ondersteuning). Ze konden ervoor kiezen maintenance en support te beëindigen maar mochten de software blijven gebruiken. Dit model bood budgetzekerheid, controle voor de langere termijn en onderhandelingsruimte.

Met de aankoop van perpetual licenties verkrijgen organisaties een asset in de vorm van gebruiksrecht in eigendom. De aanschaf is een kapitaalinvestering (CAPEX) die op de balans staat en financieel wordt afgeschreven. Het gebruiksrecht is gekoppeld aan specifieke producten - de commerciële verpakking waarin de leverancier zijn software aanbiedt - met een duidelijke vooraf gedefinieerde set functionaliteit.

De organisatie heeft hierbij controle over timing en versies. Ze kan zelf bepalen wanneer software te upgraden en nieuwe versies in gebruik te nemen. Voert de leverancier wijzigingen door in zijn productaanbod, zoals bundeling of ontbundeling van applicaties onder specifieke voorwaarden, dan heeft dat geen invloed op bestaande gebruiksrechten: het gebruiksrecht blijft van toepassing op de aangeschafte versie en functionaliteit.

Daarnaast dalen de kosten in de tijd. Door de financiële afschrijving van de aankoop dalen de jaarlijkse kosten tot alleen maintenance en support, waardoor de totale eigendomskosten over een lange periode relatief laag kunnen zijn. Leveranciers beëindigen weliswaar op termijn regulier onderhoud en reguliere support. Ze kunnen dan overgaan op duurder extended support aanbod, dat uiteindelijk ook wordt beëindigd. De software is dan end of life vanuit het perspectief van de leverancier, maar het gebruiksrecht blijft bestaan.

Wat zijn subscriptions?

In plaats van een eenmalige investering in een gebruiksrecht krijgt de organisatie bij subscriptions toegang tot de software om deze te mogen gebruiken tegen doorlopende betaling. Dit is feitelijk een verschuiving van koop naar huur van de software - een fundamentele wijziging in het licentiemodel die het verdienmodel van de leverancier verandert.

Dit betekent concreet dat organisaties geen asset meer bezitten maar een doorlopende operationele verplichting (OPEX) beheren die periodiek opnieuw onderhandeld moet worden. In plaats van specifieke producten te kopen, betalen ze voor toegang tot software die kan bestaan uit enkelvoudige applicaties of bundels van meerdere applicaties. Anders dan bij perpetual licenties, waar de kosten na afschrijving dalen, blijven de subscription kosten doorlopend op hetzelfde niveau of stijgen ze door periodieke prijsaanpassingen door de leverancier.

Drie belangrijke begrippen

In dit rapport onderscheiden we drie concepten die software leveranciers onafhankelijk van elkaar kunnen beïnvloeden:

1. **Licentiemodel:** De manier waarop de leverancier zijn verdienmodel inricht: koop (perpetual) of huur (subscription). Dit bepaalt de financiële en juridische relatie tussen organisatie en leverancier.
2. **Software/applicatie:** De feitelijke programmatuur met functionaliteit (bijvoorbeeld VMware vSphere voor virtualisatie, VMware vSAN voor storage).
3. **Product/bundel:** De commerciële verpakking waarin de leverancier zijn software aanbiedt: als losse producten die organisaties naar behoefte kunnen samenstellen, of als eenzijdig bepaalde bundels waarin meerdere applicaties zijn gecombineerd.

Waarom dit onderscheid belangrijk is:

Leveranciers kunnen bij subscription modellen alle drie deze aspecten eenzijdig wijzigen: de gebruiksvoorwaarden, de software zelf, en de manier waarop producten worden gebundeld en geprijsd.

Doordat organisaties continue moeten betalen voor toegang, verschuift de afhankelijkheidsrelatie tussen organisatie en leverancier. Waar perpetual licenties de organisatie autonomie gaven, krijgen leveranciers bij subscriptions meer instrumenten om sturing en controle uit te oefenen via drie mechanismen:

1. Eenzijdig bepaalde bundeling: Bij dit mechanisme wordt zichtbaar hoe leveranciers niet alleen de gebruiksvoorwaarden (perpetual versus subscription) maar ook de commerciële verpakking eenzijdig kunnen bepalen. Leveranciers kunnen applicaties verplicht in bundels aanbieden en het recht behouden om de samenstelling eenzijdig te wijzigen. Broadcom heeft dit model consequent doorgevoerd: organisaties kunnen geen losse producten meer afnemen en de leverancier kan functionaliteit tussen bundels en add-ons verplaatsen. Hierdoor kan functionaliteit die aanvankelijk in een bundel zat later als duurdere add-on worden aangeboden, of juist nieuwe functionaliteit wordt toegevoegd aan bestaande bundels. Dit betekent dat organisaties betalen voor gebundelde functionaliteit die mogelijk niet volledig wordt gebruikt, en verhoogt de druk om al hun afgenomen functionaliteit daadwerkelijk in gebruik te nemen, ook als die functionaliteit niet (meer) aansluit bij de behoefte van de organisatie.
2. Adoptie-prikkels: Als er sprake is van applicatie bundels dan krijgen organisaties veelal toegang tot applicaties met functionaliteit die ze niet direct nodig hebben. De leverancier stimuleert de adoptie en implementatie hiervan door trainingen, consultancy en support aan te bieden. Broadcom levert bijvoorbeeld trainingcredits mee met beperkte gebruiksduur die hiervoor ingezet kunnen worden. Indien succesvol zal de waarde van de dienstverlening van de leverancier voor de organisatie groter worden en zal de leveranciersafhankelijkheid dus toenemen.
3. Controle over upgrades: Anders dan bij perpetual licenties waar de klant zelf kan beslissen over het doorvoeren van software updates, patches en bugfixes, kunnen leveranciers bij subscriptions ook bepalen wanneer upgrades worden doorgevoerd en toegang tot de software afhankelijk stellen van het accepteren van nieuwe versies.

Daarnaast bieden subscription modellen leveranciers meer mogelijkheden tot het verkrijgen van inzicht in daadwerkelijk gebruik via ingebouwde telemetrie en monitoring, en de mogelijkheid om regelmatig licentie compliance audits uit te voeren. Dit vergroot de transparantie voor de leverancier maar verkleint de operationele ruimte voor de organisatie om zelf te bepalen wanneer en hoe software wordt ingezet.

Broadcom's specifieke mechanismen

Broadcom hanteert in de markt standaard mechanismen zoals jaarlijkse prijsverhogingen tot 10%, verplichte productmigraties binnen korte termijnen, en het SPD mechanisme (Specific Program Documentation) waarbij bij het verkrijgen van software updates ingestemd moet worden met nieuwe SPD contractvoorwaarden. In hoeverre deze mechanismen van toepassing zijn binnen specifieke rijkscontracten hangt af van de onderhandelde voorwaarden.

Ongeacht de specifieke mechanismen maakt de inherente structuur van het subscription model organisaties afhankelijk van continue betaling voor toegang. Zonder actief abonnement verliest de organisatie toegang tot de software en het recht om het te mogen gebruiken, wat resulteert in verlies van functionaliteit.

Appendix C- Virtualisatieplatformen

In deze appendix worden verschillende virtualisatie- en containerplatformen besproken aan de hand van de in 3 Besliscriteria besproken criteria. De schaal loopt van 1 tot 5, waarbij 5 vrijwel volledig voldoet aan de 3 besliscriteria en 1 vrijwel niet.

Overzicht van oplossingen

	Apache CloudStack	HPE VM Essentials	Microsoft Azure Local	Microsoft Hyper-V	Nutanix	OpenNebula	Oracle OLVM	Proxmox	Rancher Prima	Red Hat OpenShift	VMware
Kernfuncties en kenmerken van het platform	**15**	**15**	**17**	**18**	**20**	**15**	**16**	**16**	**19**	**19**	**25**
Virtualisatie/hypervisor	4	4	4	4	5	4	4	4	4	4	5
Opslag en opslagintegratie	3	3	3	3	4	3	3	4	3	3	5
(Software Defined) Netwerken	3	2	3	3	3	3	3	2	4	4	5
Bedrijfscontinuïteit	2	3	3	4	4	2	3	3	4	4	5
Beveiliging en compliance	3	3	4	4	4	3	3	3	4	4	5

	Apache CloudStack	HPE VM Essentials	Microsoft Azure Local	Microsoft Hyper-V	Nutanix	OpenNebula	Oracle OLVM	Proxmox	Rancher Prime	Red Hat OpenShift	Vmware
Beheer en automatisering	**13**	**14**	**20**	**17**	**20**	**13**	**10**	**13**	**21**	**22**	**24**
Ondersteuning en beheer van containers	3	1	4	3	4	3	1	2	5	5	4
Lifecycle management	2	2	4	4	5	2	2	3	3	4	5
Automatisering en orkestratie	3	4	4	3	4	3	2	2	5	5	5
Observability en monitoring	2	3	4	3	4	2	3	3	4	4	5
Integratie met bestaande tooling	3	4	4	4	3	3	2	3	4	4	5

	Apache CloudStack	HPE VM Essentials	Microsoft Azure Local	Microsoft Hyper-V	Nutanix	OpenNebula	Oracle OLVM	Proxmox	Rancher Prime	Red Hat OpenShift	Vmware
Bedrijfsvoering, operationele factoren en kosten	**25**	**22**	**26**	**30**	**30**	**25**	**21**	**29**	**30**	**29**	**27**
Impact op de organisatie	X	X	X	X	X	X	X	X	X	X	X
Licentie en abonnement	5	3	4	4	4	5	3	5	4	4	3
Overdraagbaarheid van licenties	5	4	4	4	5	5	4	5	5	5	4
Ondersteuningsmodel en ecosysteem	2	3	4	5	4	2	3	4	4	4	4
Migratie en exit	3	3	4	4	5	4	2	4	4	4	4
Innovatie	3	3	4	4	4	2	3	3	4	4	4
Omscholing en beschikbaarheid van talent	2	3	3	5	4	3	3	4	4	4	5
Autonomie en continuïteit van de leverancier	5	3	3	4	4	4	3	4	5	4	3
Kosten (Total Cost of Ownership)	2	4	4	4	4	3	3	4	2	1	3
Kosten Licenties en Support	5	4	3	3	1	4	4	4	2	2	1
Kosten Operationeel	1	4	4	4	5	3	3	4	2	1	2
Kosten Migratie	1	4	4	4	5	2	3	3	2	1	5

Note: De genoemde criteria zijn niet afzonderlijk gewogen. Bovenstaande scores zijn gebaseerd op de inhoud en niet op randvoorwaarden. Omdat organisaties criteria verschillend kunnen prioriteren, kan per organisatie een andere oplossing als het beste worden aangemerkt.

Total Cost of Ownership

Een exacte berekening van de TCO is niet te maken omdat hierbij veel omgevingsfactoren een rol bij spelen en dus organisatie specifiek zijn. Hierdoor is er gekozen om een scoring te geven op basis van de impact op de TCO. Om verwarring te voorkomen is de TCO schaal hetzelfde als de schaal van de capabiliteit. Bij 1 is de impact op de TCO hoog en daarmee ongunstig. Bij 5 is de impact op de TCO laag en daarmee gunstig. De TCO is opgeknipt in drie categorieën. Licenties en Support. Dit zijn de directe kosten voor het gebruik van het product. Operationele kosten zijn die van de mensen, de organisatie en de impact van de volwassenheid van het product. Bij de migratie kosten is gekeken naar de technische migratie en de complexiteit daar van, maar ook wat het betekent voor de organisatie en de mensen. Migratie tussen verschillende platform en de kosten die daar mee gepaard zijn hangen onder andere sterk van welk start en welk doel platform er wordt gekozen. In dit voorbeeld is gekozen om VMware als start platform te gebruiken.

Apache CloudStack

Apache CloudStack is een open source cloud management platform dat is ontworpen voor het bouwen en beheren van grootschalige Infrastructure as a Service (IaaS) omgevingen. CloudStack positioneert zich niet als een hypervisor of HCI platform, maar als een centrale orkestratie en beheerslaag boven bestaande compute , storage en netwerkcomponenten.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor

Voor virtualisatie ondersteunt CloudStack meerdere hypervisors, waaronder KVM (meest gebruikt in open source omgevingen), VMware ESXi, XenServer/XCP ng en in beperktere mate Hyper V. In de praktijk vormt KVM de kern van de meeste moderne CloudStack implementaties, mede door de nauwe aansluiting op Linux ecosystemen. KVM maakt gebruik van hardware assisted virtualisatie (Intel VT x, AMD V, IOMMU). KVM is breed ingezet binnen cloud omgevingen en staat bekend om zijn stabiliteit en volwassenheid. KVM is meer geschikt voor kleinschalige tot middelgrote omgevingen.

4

CloudStack abstraheert de onderliggende hypervisors en biedt centraal beheer van virtuele machines, templates, snapshots en resource allocatie. Functionaliteit zoals live migratie, high availability en resource scheduling is beschikbaar, maar sterk afhankelijk van de gekozen hypervisor en de onderliggende infrastructuur. CloudStack ondersteunt grootschalige omgevingen met duizenden hosts en virtuele machines, verdeeld over meerdere zones, pods en clusters.

Ondersteuning voor gast besturingssystemen volgt grotendeels de mogelijkheden en certificeringen van de gebruikte hypervisor en opslagstack. CloudStack wordt veel toegepast in service provider omgevingen en private clouds met een sterke focus op multi tenancy.

Opslag en opslagintegratie

CloudStack levert zelf geen opslagplatform, maar integreert met een breed scala aan externe storage backends. Opslag wordt aangeboden via primaire en secundaire storage lagen, waarbij primaire storage wordt gebruikt voor draaiende virtuele machines en secundaire storage voor templates, ISO's en snapshots.
Ondersteunde opslagoplossingen omvatten NFS, iSCSI, Fibre Channel en software defined storage zoals Ceph. CloudStack biedt abstrahering en lifecycle management van volumes, maar data services zoals deduplicatie, compressie en encryptie zijn volledig afhankelijk van de onderliggende storage technologie.
Functionaliteit zoals snapshots, cloning en thin provisioning is beschikbaar wanneer de storage backend dit ondersteunt. Replicatie en databescherming worden doorgaans gerealiseerd via externe storage oplossingen of backup software. CloudStack fungeert hierbij als orkestratielaag en niet als data platform.

3

(Software Defined) Netwerken

Netwerkfunctionaliteit is een van de kernsterktes van CloudStack. Het platform ondersteunt zowel traditionele netwerkmodellen als uitgebreide Software Defined Networking concepten, afhankelijk van de gekozen netwerkarchitectuur.
CloudStack ondersteunt verschillende netwerktypen, waaronder basic en advanced networking, met ondersteuning voor VLAN's, VXLAN, en overlay netwerken. Integratie met virtual routers, firewalls, load balancers en VPN diensten is standaard beschikbaar. Netwerkdiensten kunnen per tenant of per netwerk worden aangeboden.

4

Microsegmentatie, NAT, DHCP, DNS en load balancing zijn geïntegreerd in het platform, vaak via virtuele netwerkappliances. Voor complexere use cases kan CloudStack integreren met externe SDN oplossingen en fysieke netwerkapparatuur.
De netwerkarchitectuur is expliciet ontworpen voor multi tenancy en self service, wat CloudStack aantrekkelijk maakt voor service provider achtige omgevingen.

Bedrijfscontinuïteit

CloudStack ondersteunt hoge beschikbaarheid voor virtuele machines door middel van monitoring en automatische herstart op andere hosts bij uitval. De exacte hersteltijd en mogelijkheden zijn afhankelijk van de gebruikte hypervisor, gedeelde opslag en netwerkconfiguratie. Voor noodherstel biedt CloudStack geen volledig geïntegreerde end to end oplossing. Replicatie en failover worden doorgaans gerealiseerd via opslag replicatie, externe backup oplossingen en aanvullende automatisering. Orkestratie van herstelprocessen kan worden ingericht via CloudStack API's en scripts, maar vereist doorgaans maatwerk.
De bedrijfscontinuïteit is daarmee sterk afhankelijk van architectuurkeuzes en operationele discipline.

2

Beveiliging en compliance

Beveiliging binnen CloudStack is gebaseerd op een combinatie van platformfunctionaliteit en integratie met externe systemen. Het platform ondersteunt Role Based Access Control (RBAC), multi tenancy en strikte scheiding van resources per account, project of domein. Authenticatie kan worden geïntegreerd met LDAP en Active Directory. Netwerkbeveiliging wordt geleverd via virtuele firewalls, security groups en network ACL's. Audit logging en quota beheer ondersteunen compliance doelstellingen.
Encryptie van data at rest en in transit is mogelijk, maar afhankelijk van de gebruikte storage en netwerkcomponenten. CloudStack hanteert geen volledig secure by default model; hardening en patching van hypervisors en infrastructuur vallen onder de verantwoordelijkheid van de beheerorganisatie.

3

Beheer en automatisering

Ondersteuning en beheer van containers

CloudStack biedt geen geïntegreerd containerplatform, maar biedt via plug-ins de mogelijkheid om Kubernetes clusters als uit te rollen en te beheren via CloudStack. Deze aanpak maakt het mogelijk om containers te draaien binnen een CloudStack omgeving op basis van verschillende Kubernetes distributies, maar biedt geen diep geïntegreerde container ervaring zoals Kubernetes native platforms.

3

Lifecycle management

Lifecycle management binnen CloudStack richt zich op het beheer van virtuele machines, templates, snapshots en netwerken. Upgrades van het CloudStack platform zijn gestructureerd, maar lifecycle management van hypervisors, firmware en hardware valt buiten de scope van het platform.
Dit biedt flexibiliteit in infrastructuurkeuze, maar verhoogt de operationele complexiteit en verantwoordelijkheid voor de beheerorganisatie.

2

Automatisering en orkestratie
CloudStack biedt uitgebreide automatiseringsmogelijkheden via REST APIs, CLI tools en declaratieve templates. Self service provisioning van virtuele machines, netwerken en opslag is een kernfunctie van het platform.
Integratie met externe automatiseringstools zoals Ansible en Terraform is gebruikelijk, waarbij CloudStack fungeert als orchestrator voor infrastructuurresources. De automatisering is sterk gericht op IaaS use cases en minder op applicatie level orkestratie.

3

Observability en monitoring
CloudStack biedt basisfunctionaliteit voor monitoring van hosts, virtuele machines en capaciteit. Metrieken en statusinformatie zijn beschikbaar via de webinterface en APIs.
Voor geavanceerde observability, logging en performance analyse is integratie met externe monitoring platformen gangbaar. CloudStack zelf biedt beperkte diepgaande analytics in vergelijking met commerciële platforms.

2

Integratie in bestaande beheersystemen
CloudStack is ontworpen voor integratie. Via open API's en een modulair ontwerp kan het platform worden gekoppeld aan bestaande billing , monitoring , identity en backup systemen. Dit maakt CloudStack populair bij service providers en organisaties met maatwerkbehoeften.
Het ecosysteem is grotendeels open source gedreven en minder gestandaardiseerd dan dat van commerciële leveranciers.

3

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
CloudStack vraagt doorgaans aanzienlijke kennis van Linux, netwerken en cloudarchitecturen. Daartegenover staat een hoge mate van controle en flexibiliteit, vooral in multi tenant omgevingen. De manier waarop met CloudStack beheerd en ontwikkeld wordt is aanzienlijk anders dan met een regulier virtualisatieplatform, waardoor de impact op de organisatie in veel gevallen aanzienlijk is.

TB

Licentie en abonnement
Apache CloudStack is volledig open source en kent geen licentiekosten. Commerciële ondersteuning wordt aangeboden door derde partijen en system integrators.
Dit verlaagt directe softwarekosten, maar verlegt de focus naar operationele inzet en expertise.

5

Overdraagbaarheid van licenties
Door het open source karakter zijn er geen licentiebeperkingen. CloudStack kan vrij ingezet worden in on premises, private cloud en service provider omgevingen.

5

Ondersteuningsmodel en ecosysteem
Ondersteuning is beschikbaar via commerciële partijen en de open source community. Het ecosysteem is actief, maar kleiner en minder gecentraliseerd dan dat van marktleiders als Red Hat of VMware.

2

Migratie en exit

Migratie naar CloudStack vereist doorgaans herontwerp van netwerk en opslag architecturen en conversie van virtuele machines. Exit lijkt relatief eenvoudig doordat gebruik wordt gemaakt van standaard hypervisors en open technologieën, maar vergt in de meeste gevallen ook herontwerp om de functies die CloudStack biedt over te nemen.

3

Innovatie

Innovatie binnen CloudStack is community gedreven en gericht op stabiliteit, schaalbaarheid en netwerkfunctionaliteit. De ontwikkelsnelheid is stabiel, maar minder agressief dan bij commercieel gedreven platforms.

3

Omscholing en beschikbaarheid van talent

CloudStack expertise is niche en vooral te vinden bij service providers en open source gerichte organisaties. Omscholing is vaak noodzakelijk voor teams met een traditionele enterprise virtualisatieachtergrond.

2

Autonomie en continuïteit van de leverancier

Het Apache projectmodel biedt hoge autonomie en voorkomt leverancierslock in. Continuïteit is gekoppeld aan community activiteit en commerciële ondersteuning, maar niet aan één enkele leverancier.

5

Kosten (Total Cost of Ownership)

Er hoeven geen licenties te worden afgenomen voor CloudStack. Support kan eventueel via een 3rd party worden afgenomen. Operationele kosten kunnen hoger uitvallen door complexiteit en benodigde expertise. Automatisering zal je grotendeels zelf moeten opzetten. Voor organisaties met ervaring in grootschalige IaaS omgevingen kan CloudStack echter een kosteneffectieve en flexibele oplossing zijn. Migratie naar CloudStack kan complex zijn omdat er geen standaard tooling is om dit te automatiseren.

2

HPE Morpheus VM Essentials

HPE Morpheus VM Essentials is een softwarematige virtualisatie- en cloudmanagementoplossing die zich richt op het beheren en consumeren van virtuele machines binnen on premises en hybride omgevingen. Morpheus VM Essentials is een controle plane die bovenop bestaande infrastructuur en hypervisors opereert. HPE is Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor

HPE Morpheus VM Essentials ondersteunt meerdere hypervisors parallel (waaronder KVM gebaseerde platforms en bestaande VMware omgevingen) en biedt één centraal beheer- en consumptiemodel. De focus ligt niet op hypervisor specifieke optimalisaties, maar op uniforme provisioning, governance en lifecyclebeheer van VM's over verschillende platformen heen. Hierdoor is het platform geschikt voor organisaties die hun virtualisatielaag willen vereenvoudigen of transformeren zonder directe infrastructuurvervanging. Het kan daarmee gebruikt worden om te migreren van VMware naar KVM(Kernel based Virtual Machine), een open source hypervisor die onderdeel is van de Linux kernel.

KVM maakt gebruik van hardware assisted virtualisatie (Intel VT x, AMD V, IOMMU). KVM is breed ingezet binnen cloud omgevingen en staat bekend om zijn stabiliteit en volwassenheid. KVM is meer geschikt voor kleinschalige tot middelgrote omgevingen. De schaalbaarheid is beperkter dan bij marktleidende virtualisatieplatformen en richt zich vooral op enkele clusters binnen één of enkele locaties, al is Morpheus wel in staat om breder ingezet te worden. Ondersteuning voor gangbare gast besturingssystemen, zoals Linux distributies en Windows Server, is beschikbaar. Voor zware of specialistische enterprise applicaties is aanvullende validatie nodig, met name op het gebied van performance, beschikbaarheid en ondersteuning.
N.B. voor de evaluatie van de verschillende onderdelen wordt uitgegaan van de meegeleverde KVM-gebaseerde hypervisor. Wanneer organisaties VMware toepassen als onderliggende hypervisor, zijn de mogelijkheden van dat platform van toepassing.

4

Opslag en opslagintegratie

HPE Morpheus VM Essentials bevat zelf geen opslaglaag en levert geen software-defined storage. Opslag wordt volledig geleverd door de onderliggende infrastructuur en hypervisorplatformen waarop Morpheus wordt ingezet. Dit sluit aan bij de traditionele HPE architectuur, waarin rekenkracht en opslag logisch gescheiden zijn.
Het platform integreert met bestaande storage-oplossingen via de hypervisor- en cloudintegraties en biedt abstrahering op consumptieniveau, bijvoorbeeld via catalogi en policies. Daarbij integreert het goed met het HPE opslagportfolio, zoals HPE Alletra, Primera en Nimble Storage. Opslag wordt ontsloten via gangbare enterprise protocollen zoals iSCSI, Fibre Channel en NFS. Hierdoor kunnen bestaande SAN en NAS omgevingen worden hergebruikt, inclusief bijbehorende functionaliteit zoals snapshots, replicatie en performance tiering.

3

Datadiensten zoals replicatie, snapshots, encryptie en performance-optimalisatie blijven de verantwoordelijkheid van de gebruikte storage- en virtualisatieplatformen. Data protection en continuïteit worden daarom niet door Morpheus zelf afgedwongen, maar kunnen wel georkestreerd worden via integraties met bestaande backup- en recoveryoplossingen en automatiseringsworkflows.

(Software Defined) Netwerken

Netwerkfunctionaliteit binnen HPE Morpheus VM Essentials wordt geleverd door de onderliggende netwerk- en virtualisatieplatformen.
Morpheus fungeert als orkestratie- en automatiseringslaag en configureert netwerkcomponenten via bestaande API's en integraties.
Het platform ondersteunt het modelleren van netwerkconfiguraties als onderdeel van provisioning templates en policies, maar biedt geen eigen SDN functionaliteit. Segmentatie, microsegmentatie en netwerkbeveiliging zijn afhankelijk van de gebruikte hypervisor en netwerkstack.

2

Netwerkfunctionaliteit voor de KVM hypervisor is gebaseerd op standaard Linux en KVM netwerkcomponenten. Virtuele switches, VLAN ondersteuning en basis netwerkisolatie zijn beschikbaar via de hypervisor.
Voor geavanceerde netwerkfunctionaliteit, zoals microsegmentatie, uitgebreide netwerkvirtualisatie of multi tenant overlay netwerken, is het platform afhankelijk van externe netwerkoplossingen. Het beheer van het netwerk ligt grotendeels buiten het virtualisatieplat form en volgt de bestaande fysieke en logische netwerkarchitectuur.
Deze aanpak zorgt voor eenvoud en voorspelbaarheid, maar biedt minder mogelijkheden voor cloud achtige self service, uitgebreide automatisering of geïntegreerde netwerkbeveiliging zonder aanvullende tooling.

Bedrijfscontinuïteit

HPE Morpheus VM Essentials levert zelf geen hoge-beschikbaarheids- of disaster-recoverymechanismen. Deze functies zijn volledig afhankelijk van de mogelijkheden van de onderliggende infrastructuur en hypervisors.
Morpheus kan wel worden ingezet om failover-scenario's, herstelprocedures en herdeployments te automatiseren en te standaardiseren, waardoor operationele continuïteit verbetert zonder dat het platform zelf een single point of failure vormt.
De KVM hypervisor biedt basisfunctionaliteit voor hoge beschikbaarheid op virtuele machine niveau, afhankelijk van de configuratie van de KVM cluster en het gebruik van gedeelde opslag. Bij uitval van een host kunnen virtuele machines automatisch opnieuw worden gestart op andere hosts binnen het cluster.

3

Live migratie van virtuele machines is mogelijk binnen de beperkingen van KVM en gedeelde storage. Geavanceerde disaster recovery scenario's, zoals geautomatiseerde site failover of orchestratie van herstelprocessen, zijn niet standaard onderdeel van het platform en vereisen aanvullende oplossingen, bijvoorbeeld via storage replicatie of third party tooling.
Voor organisaties met strikte RPO en RTO eisen vraagt dit om aanvullende architectuurkeuzes en operationele afspraken.

Beveiliging en compliance

Beveiliging binnen HPE Morpheus VM Essentials is primair gericht op governance, toegangsbeheer en auditability. Het platform ondersteunt Role Based Access Control (RBAC), tenant-scheiding, logging en policy-based provisioning.
Integratie met bestaande identity-oplossingen (zoals LDAP en Active Directory) maakt centrale authenticatie en autorisatie mogelijk.
Infrastructuur- en databeveiliging (encryptie, netwerkbeveiliging, platform-hardening) vallen buiten Morpheus zelf en blijven onderdeel van de onderliggende platformen.

3

Beveiliging rondom virtualisatie is gebaseerd op standaard Linux securitymechanismen en enterprise best practices. Encryptie van data at rest en data in transit is mogelijk, maar sterk afhankelijk van configuratie en onderliggende infrastructuur.
Compliance monitoring, auditing en logging worden doorgaans ingevuld via bestaande security en monitoringoplossingen binnen de organisatie, in plaats van via native platformfunctionaliteit.

Beheer en automatisering

Ondersteuning en beheer van containers

HPE Morpheus VM Essentials richt zich primair op virtuele machines en biedt geen geïntegreerde container of Kubernetes oplossing. Containerplatformen worden buiten het virtualisatieplatform beheerd, bijvoorbeeld via afzonderlijke Kubernetes clusters of cloud native diensten.
Hierdoor is het platform minder geschikt voor organisaties die sterk inzetten op container first of cloud native architecturen, maar passend voor omgevingen waarin virtuele machines dominant blijven.

1

Lifecycle management

Lifecycle management binnen Morpheus VM Essentials richt zich op het applicatieniveau. Het platform ondersteunt het beheren van VM-levenscycli, van uitrol tot uit dienst nemen van VMs, inclusief beleid, quota en kostenallocatie.
Lifecycle management van de virtualisatielaag is functioneel, maar beperkt. Updates van hypervisor en managementcomponenten worden doorgaans handmatig of semi geautomatiseerd uitgevoerd.

2

Firmware en hardware updates vallen buiten de scope van het platform en worden beheerd via HPE specifieke tools zoals HPE iLO en HPE OneView. Dit vereist duidelijke operationele processen om consistentie en stabiliteit te waarborgen.

Automatisering en orkestratie

Automatisering is een kernfunctie van HPE Morpheus VM Essentials. Het platform biedt uitgebreide mogelijkheden voor het modelleren van applicaties, uitrolstromen en operationele activiteitn via workflows, blueprints en API-integraties.
Integratie met tools zoals Terraform, Ansible en CI/CD-platformen maakt het mogelijk om Morpheus in te passen in bestaande DevOps- en infrastructuur-as-code-processen.

4

Observability en monitoring

Morpheus VM Essentials biedt inzicht in resourcegebruik, kosten en status van workloads, maar is geen volwaardige monitoring of observability oplossing.
Diepgaande performance monitoring en analyse worden doorgaans geleverd door de onderliggende virtualisatieplatformen of gespecialiseerde third party tooling. Geavanceerde correlatie, capaciteitsplanning en predictive analytics vereisen aanvullende tooling buiten het platform.

3

Integratie in bestaande beheersystemen

Een belangrijk ontwerpprincipe van HPE Morpheus VM Essentials is brede integratie. Het platform is hypervisor- en hardware-agnostisch en integreert met bestaande ITSM-, monitoring-, automation- en financiële systemen.
Hierdoor kan VM Essentials worden ingezet als centrale cloudmanagementlaag zonder bestaande beheerprocessen volledig te vervangen.

4

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

HPE Morpheus VM Essentials kan de complexiteit van multi hypervisor omgevingen reduceren en biedt een uniform consumptiemodel. De operationele verantwoordelijkheid voor infrastructuur blijft echter bij de organisatie zelf en daarmee is hangt de impact op de organisatie ook af van of alleen KVM of ook VMware gebruikt wordt.

TB

Voor organisaties met ervaring in Linux en HPE omgevingen is weinig aanpassing vereist. Wanneer alleen van KVM gebruik gemaakt wordt, kan het platform functioneel beperkend zijn en moet veel gerealiseerd worden met third party tooling hetgeen aanpassingen vergt in de architectuur en de kennisopbouw van deze tooling.

Licentie en abonnement

HPE Morpheus VM Essentials wordt geleverd als software abonnement. De licentie is losgekoppeld van hardware en infrastructuur en biedt flexibiliteit in inzet en schaal. Indien VMware toegepast wordt, dient hiervoor een aparte licentie aangeschaft worden.
De licenties zijn gebaseerd op een per socket model, waarbij het aantal cores niet uitmaakt en kunnen afgesloten worden voor 1, 3 of 5 jaar.

3

Overdraagbaarheid van licenties

Licenties voor Morpheus VM Essentials zijn niet gebonden aan specifieke hardware of locaties en kunnen in verschillende omgevingen worden ingezet, zolang aan de licentievoorwaarden wordt voldaan.

4

Ondersteuningsmodel en ecosysteem

Ondersteuning wordt geleverd via HPE supportmodellen en partners. De kwaliteit en diepgang van ondersteuning zijn afhankelijk van het gekozen supportniveau.
Ondersteuning wordt geleverd door HPE en partners. Het ecosysteem rond Morpheus bestaat uit integraties met infrastructuur , cloud en automation leveranciers, maar is kleiner en minder gestandaardiseerd dan dat van gevestigde hypervisorplatformen.

3

Migratie en exit

Morpheus VM Essentials ondersteunt migratie en transformatiestrategieën door parallel beheer van meerdere platformen mogelijk te maken. Dit kan de afhankelijkheid van één specifieke hypervisor verminderen.
Exit uit Morpheus is relatief eenvoudig, omdat applicaties niet afhankelijk zijn van Morpheus specifieke infrastructuurcomponenten, maar daarmee is een exit uit de onderliggende infrastructuur nog niet geregeld mocht dit nodig zijn.
Migratie naar de KVM hypervisor vereist conversie van virtuele machines naar KVM compatibele formaten en wordt doorgaans uitgevoerd met third party migratietools.

3

Innovatie

De ontwikkeling van Morpheus richt zich op cloudmanagement, automatisering en multi-platform governance. Innovatie zit vooral in abstrahering en orkestratie, niet in infrastructuurfeatures.
HPE positioneert de KVM-hypervisor als pragmatisch en stabiel. Innovatie richt zich vooral op vereenvoudiging en kostenbeheersing, in plaats van snelle introductie van nieuwe cloud native functionaliteit.

3

Omscholing en beschikbaarheid van talent

Morpheus VM Essentials vereist kennis op het gebied van cloud governance en automatisering. De leercurve is beperkter dan bij volledige infrastructuurplatformen, maar kennis is minder breed beschikbaar dan bij marktleidende hypervisors en vereist additionele kennis. Doordat HPE Morpheus VM Essentials zich met name richt op governance en automatisering en daarmee op relatief eenvoudige virtualisatieomgevingen, zonder uitgebreide netwerk- en opslagfunctionaliteit en geen standaardondersteuning voor containers, zijn

3

daarvoor alternatieve oplossingen nodig waarvoor apart expertise opgebouwd moet worden.
Kennis van KVM en Linux is breed beschikbaar in de markt. Specifieke kennis van HPE VM Essentials is beperkter, maar sluit goed aan bij bestaande Linux en HPE expertise.

Autonomie en continuïteit van de leverancier
HPE Morpheus VM Essentials kan volledig on premises worden ingezet zonder verplichte cloud connectiviteit, wat de autonomie van de afnemer vergroot.
HPE is een gevestigde leverancier met een lange geschiedenis in enterprise infrastructuur, wat de continuïteit van het platform ondersteunt.
HPE heeft voor hun private cloud oplossing een groot contract afgesloten met de Amerikaanse overheid, wat de continuïteit bevordert.
Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten zij levert.

3

Kosten (Total Cost of Ownership)
Het eenvoudiger licentiemodel en gebruik van de KVM-hypervisor kan leiden tot lagere TCO dan uitgebreide enterprisevirtualisatieplatformen, met name in omgevingen waar minder behoefte is aan geavanceerde cloudachtige functionaliteit. Als gebruik gemaakt wordt van VMware als hypervisor gaan de licentiekosten initieel omhoog, omdat deze additioneel zijn. De mogelijkheid om vervolgens te optimaliseren en het gebruik van VMware te verminderen als dit voorheen het gebruikte platform was, maakt kostenbesparingen mogelijk. De impact op de organisatie is beperk omdat de omgeving relatief makkelijk te beheren is. Als er al virtualisatie kennis aanwezig is, is de stap klein. Tevens is de beheer last per unit relatief laag. Migratie vanaf Vmware is eenvoudig door een gestandaardiseerde aanpak.

4

Microsoft Azure Local

Azure Local is Microsofts on premises en edge virtualisatie en HCI platform, gebaseerd op Windows Server en Hyper V, en sterk geïntegreerd met Azure diensten. Het platform is ontworpen voor het draaien van virtuele machines en containers in het datacenter of aan de edge, met centrale aansturing en extensies vanuit Azure. Een versie die geen connectiviteit met de cloud vereist is in ontwikkeling (Preview).
Microsoft is Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor
De hypervisorlaag wordt geleverd door Hyper V, die gebruikmaakt van hardware assisted virtualisatie (Intel VT x, AMD V, SLAT) en geavanceerde CPU , geheugen en I/O optimalisaties. Hyper V ondersteunt NUMA bewustzijn, live migratie van virtuele machines en dynamisch geheugenbeheer, waardoor resources efficiënt benut kunnen worden over meerdere hosts.

4

Azure Local schaalt van kleine 2 node clusters tot grotere clusters (momenteel tot 16 nodes per cluster, afhankelijk van gevalideerde hardware). Clusterbeheer gebeurt centraal via Windows Failover Clustering, met uitbreiding naar Azure voor beheer, monitoring en lifecycle integratie. Het platform ondersteunt een breed scala aan gast besturingssystemen, waaronder Windows Server en diverse Linux distributies. Voor workloads zoals SQL Server en SAP zijn specifieke configuratie en hardwarevereisten van toepassing.

Opslag en opslagintegratie
Opslag in Azure Local wordt geleverd via Storage Spaces Direct (S2D), waarmee lokale disks van meerdere hosts worden samengevoegd tot één software defined storage pool. S2D ondersteunt verschillende disktypes (NVMe, SSD, HDD) en maakt gebruik van resiliency mechanismen zoals mirroring en parity om data te beschermen tegen schijf-en node-uitval.

3

De opslag wordt beheerd met volumes op basis van ReFS, wat integratie biedt met functionaliteit zoals block cloning en snelle herstelacties. Data wordt automatisch verdeeld over de nodes in het cluster, wat hoge beschikbaarheid en consistente performance mogelijk maakt.

Encryptie van data at rest is standaard beschikbaar via BitLocker, met integratie met externe key opslag (bijvoorbeeld Azure Key Vault). Snapshots en back ups worden doorgaans verzorgd via Microsoft of third party back upoplossingen die integreren met VSS en Hyper V. Azure Local richt zich primair op HCI opslag; integratie met externe SAN oplossingen is mogelijk, maar valt buiten het kernontwerp van het platform en wordt minder diepgaand ondersteund dan bij traditionele SAN gebaseerde architecturen.

(Software Defined) Netwerken

Netwerkfunctionaliteit in Azure Local is gebaseerd op Software Defined Networking (SDN) binnen Windows Server. Virtuele switches, VLANs en netwerk QoS zijn standaard beschikbaar via Hyper V.
Voor geavanceerdere scenario's biedt Azure Local ondersteuning voor SDN componenten zoals: 1) Virtuele netwerken en netwerkvirtualisatie, 2) Load balancing via Software Load Balancer (SLB), 3) Microsegmentatie en netwerkbeveiliging via Network Security Groups (NSG achtige concepten)

3

Integratie met Azure maakt hybride netwerkscenario's mogelijk, bijvoorbeeld via VPN of ExpressRoute, waarmee on premises workloads kunnen communiceren met Azure Virtual Networks. In vergelijking met gespecialiseerde SDN oplossingen is de netwerklaag functioneel sterk geïntegreerd met het OS, maar minder uitgebreid in multi tenant en multi site overlay scenario's.

Bedrijfscontinuïteit

Azure Local biedt hoge beschikbaarheid via Failover Clustering. Bij uitval van een host worden virtuele machines automatisch opnieuw gestart op andere nodes binnen het cluster. De herstarttijd is afhankelijk van workload en configuratie, maar is doorgaans beperkt tot enkele minuten.

3

Live Migration maakt het mogelijk om virtuele machines zonder downtime te verplaatsen tussen hosts voor onderhoud of load balancing. Voor site niveau noodherstel kan Azure Site Recovery worden ingezet, waarmee replicatie van virtuele machines naar Azure mogelijk is. Dit maakt Azure een secundaire locatie voor disaster recovery, met configureerbare recovery points.
Stretch clusters zijn mogelijk met specifieke gevalideerde hardware en netwerklatency eisen, maar worden vooral toegepast in edge en regionale scenario's.

Beveiliging en compliance

Beveiliging is diep geïntegreerd in Azure Local via Windows Server security mogelijkheden. Identiteit en toegang worden geregeld via Active Directory, met optionele integratie met Entra ID (voorheen Azure Active Directory) voor hybride identiteitsmodellen.
Role Based Access Control (RBAC) is beschikbaar via Windows en Azure rollen. Just Enough Administration (JEA) en Just In Time (JIT) access kunnen worden toegepast om beheerdersrechten te beperken.

4

Encryptie van data at rest (BitLocker) en data in transit (SMB encryption, TLS) is standaard beschikbaar. Security monitoring en compliance rapportage kunnen worden uitgebreid met Azure Defender en Azure Policy, waarmee policies centraal kunnen worden afgedwongen en gecontroleerd. Dit vereist echter wel verbinding met de Azure cloud.

Beheer en automatisering

Ondersteuning en beheer van containers

Azure Local ondersteunt containers via Azure Kubernetes Service on Azure Local (AKS on Azure Local). Dit biedt een on premises Kubernetes distributie die sterk lijkt op AKS in Azure, inclusief centraal beheer via de Azure control plane.
AKS on Azure Local is CNCF conform en gericht op consistentie tussen on premises en cloud. Virtuele machines en Kubernetes clusters worden echter grotendeels afzonderlijk beheerd; er is beperkte gezamenlijke lifecycle integratie op infrastructuurniveau.

4

Lifecycle management

Lifecycle management van Azure Local wordt verzorgd via een combinatie van Windows Admin Center en Azure integratie. Updates voor het besturingssysteem, drivers en firmware kunnen gecoördineerd worden uitgerold via Cluster Aware Updating (CAU), waardoor rolling upgrades mogelijk zijn met minimale impact op workloads.

Azure kan gebruikt worden voor update insights, compliance status en advisering, maar de daadwerkelijke uitvoering van updates vindt lokaal plaats. Declaratief lifecycle management is beperkter dan bij sommige geïntegreerde private cloud suites.

4

Automatisering en orkestratie

Automatisering is mogelijk via PowerShell, Windows Admin Center en Azure Resource Manager (ARM) templates voor hybride scenario's. Daarnaast is integratie met tools zoals Ansible en Terraform mogelijk, zij het vaak via generieke Hyper V of Azure providers.
De focus ligt op script- en policy-gedreven automatisering, met sterke integratie in het bredere Microsoft ecosysteem.

4

Observability en monitoring

Monitoring van Azure Local kan lokaal plaatsvinden via Windows Admin Center en Performance Monitor, en centraal via Azure Monitor. Metrics voor CPU, geheugen, storage en netwerk worden verzameld en gevisualiseerd in Azure, met ondersteuning voor alerts en dashboards.

Log-analyse en geavanceerde correlatie zijn mogelijk via Log Analytics en integratie met SIEM-oplossingen zoals Microsoft Sentinel. Voor organisaties zonder Azure-koppeling is men aangewezen op lokale of third party monitoringtools.

4

Integratie in bestaande beheersystemen

Azure Local integreert sterk met Microsoft gebaseerde beheer en securitytools. Back up, monitoring en security worden vaak ingevuld met oplossingen uit het Azure ecosysteem, aangevuld met partners zoals Veeam, Commvault en Rubrik.
De integratie met niet Microsoft tooling is aanwezig, maar minder breed gecertificeerd dan bij sommige traditionele virtualisatieplatformen.

4

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

Voor organisaties met bestaande Windows Server en Azure kennis is de leercurve beperkt. Voor organisaties die uit een niet Microsoft ecosysteem komen, is waarschijnlijk omscholing nodig.

TB

Licentie en abonnement
Azure Local wordt afgenomen via een abonnementsmodel per core, met verplichte registratie in Azure. Dit abonnement dekt het gebruiksrecht van de HCI software; Windows Server gastlicenties en aanvullende Azure diensten worden apart gelicenseerd.

4

Overdraagbaarheid van licenties
Licenties zijn gekoppeld aan het Azure abonnement en niet vrij overdraagbaar naar andere cloud -of on- premises platforms. Wel is hybride inzet mogelijk door workloads te combineren met Azure.

4

Ondersteuningsmodel en ecosysteem
Ondersteuning verloopt via Microsoft, met één supportmodel voor zowel on premises als Azure componenten. De kwaliteit van ondersteuning is sterk afhankelijk van contractvorm (bijvoorbeeld Unified Support).

Het ecosysteem rondom Azure Local groeit, maar is kleiner dan dat van traditionele marktleiders in virtualisatie. Doordat er een grote mate van overeenkomst zit tussen Azure Local en Azure, is ook het bredere Azure ecosysteem deels in te schakelen.

4

Migratie en exit
Migratie naar Azure Local kan plaatsvinden via Hyper-V-migratietools en third-party oplossingen. Migratie naar Azure wordt expliciet ondersteund via Azure Site Recovery en Azure Migrate.

Een exit naar andere platformen is mogelijk, maar vereist herinrichting van applicaties en beheer, met name door de sterke integratie met Azure diensten.

4

Innovatie
Microsoft investeert actief in Azure Local als verlengstuk van Azure, met focus op hybride cloud, edge computing en integratie met AI en data diensten. Innovatie vindt grotendeels plaats in Azure, waarna functionaliteit wordt doorvertaald naar Azure Local.

4

Omscholing en beschikbaarheid van talent
Kennis van Windows Server en Azure is breed beschikbaar in de markt. Microsoft biedt uitgebreide documentatie, online trainingen en certificeringen. Specifieke AzureLocal-expertise is echter nog minder wijdverbreid dan algemene Azure-kennis.

4

Autonomie en continuïteit van de leverancier
Azure Local vereist periodieke connectiviteit met Azure voor registratie en facturatie. Bij langdurig wegvallen van deze connectiviteit kan dit gevolgen hebben voor ondersteuning en compliance, maar niet direct voor het draaien van applicaties.
Azure Local for Disconnected Operations is in ontwikkeling (Preview) en vereist geen connectiviteit met Azure. Deze optie zal minder rijk in functie zijn. De licentiestructuur van deze optie is nog onbekend.

Microsoft is een zeer kapitaalkrachtige leverancier met een lange termijnstrategie op hybride cloud, wat de continuïteit van het platform hoog maakt.

3

Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten zij levert. Het stoppen van diensten zou met name invloed hebben op hybride diensten vanuit de cloud, ondersteuning en toekomstige updates. Daarnaast kan er op den duur geen licentiecontrole meer uitgevoerd worden, waardoor geen nieuwe applicaties uitgerold kunnen worden.

Kosten (Total Cost of Ownership)
Hoewel het abonnementsmodel terugkerende kosten introduceert, kunnen besparingen ontstaan door standaardisatie, integratie met bestaande Microsoftlicenties en vereenvoudigd beheer in hybride omgevingen. Voor beheerders met Azure kennis is het een ideaal platform. Migratie is relatief eenvoudig door gebruikt te maken van standaard tooling.

4

Microsoft Hyper-V

Microsoft Hyper-V is de hypervisor die geïntegreerd is in Windows Server en Microsoft Azure Local (voorheen Azure Stack HCI). Als hypervisor is Hyper-V al lang beschikbaar en stabiel, maar het is relatief beperkt in functie ten opzichte van een de marktleiders. Innovatie is beperkt, omdat die vooral gericht is op Azure Local.
Microsoft is Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor
Microsoft Hyper-V is de hypervisor die geïntegreerd is in Windows Server en Microsoft Azure Local (voorheen Azure Stack HCI). Hyper-V biedt een stabiel en volwassen virtualisatieplatform met sterke integratie met Microsoft-technologieën zoals Active Directory, Windows Server Failover Clustering en System Center. De hypervisor ondersteunt hardware-assisted virtualisatie (Intel VT-x, AMD-V), Second Level Address Translation (SLAT), NUMA en SR-IOV.

4

Hyper-V ondersteunt live migratie, storage live migration en replica technologie voor het verplaatsen van workloads zonder downtime. Clusters kunnen tot 64 nodes omvatten en een cluster kan maximaal 8000 virtuele machines hosten. Centraal beheer is mogelijk via Failover Cluster Manager, Windows Admin Center en System Center Virtual Machine Manager (SCVMM).

Gast OS ondersteuning omvat alle Windows varianten, de meeste Linux distributies (met geïntegreerde LIS drivers) en FreeBSD. Hyper-V biedt gecertificeerde ondersteuning voor onder andere Oracle RAC en SAP, indien aan de hardware eisen voldaan wordt.

Opslag en opslagintegratie
Hyper-V ondersteunt verschillende opslagmodellen. Traditionele SAN- en NAS-oplossingen kunnen worden aangesloten via Fibre Channel, iSCSI en SMB 3.0. SMB 3.0 biedt ondersteuning voor functies zoals Multichannel, RDMA en Continuous Availability, waardoor het geschikt is voor enterprise workloads.
Lokale opslag kan worden ingezet in combinatie met Storage Spaces Direct (S2D), waarmee een software-defined storage-laag wordt gerealiseerd over meerdere hosts. S2D is een kerncomponent van Azure Stack HCI en maakt gebruik van lokale disks (NVMe, SSD, HDD) om een gedeelde, schaalbare en fouttolerante storagepool te creëren.
Optimalisatie van opslag vindt plaats via caching (bijvoorbeeld NVMe-cache in S2D), thin provisioning en automatische herverdeling van data binnen storage pools. Bij heterogene storageconfiguraties bepaalt, net als bij andere HCI-oplossingen, de minst presterende component de maximale performance.

3

(Software Defined) Netwerken
Hyper-V maakt gebruik van Hyper-V Virtual Switch voor netwerkvirtualisatie. Deze virtual switch ondersteunt VLANs, NIC teaming, QoS en extensies voor monitoring en security. Netwerkbeheer is sterk geïntegreerd met het onderliggende Windows-netwerkstack. Voor meer geavanceerde software-defined networking biedt Microsoft Software Defined Networking (SDN) binnen Windows Server. Dit omvat

3

te automatiseren, met ondersteuning voor overlays, netwerksegmentatie en integratie met Azure-netwerkdiensten. Integratie met containers en Kubernetes-netwerken is mogelijk via Azure Kubernetes Service (AKS) op Azure Stack HCI.
Samenwerking met Cisco ACI is mogelijk via L2/L3 bridging maar er is geen diepe integratie met inzicht in ACI vanuit Hyper-V.

Bedrijfscontinuïteit□
Hyper-V biedt hoge beschikbaarheid via Failover Clustering. Virtuele machines worden automatisch herstart op andere hosts bij uitval van hardware. In combinatie met Live Migration is het mogelijk om onderhoud uit te voeren met minimale impact op applicaties.
Voor noodherstel kan Hyper-V Replica worden ingezet, waarmee virtuele machines asynchroon worden gerepliceerd naar een secundaire locatie. Herstelpunten (recovery points) kunnen worden geconfigureerd met verschillende retentie-instellingen om bescherming te bieden tegen datacorruptie.

4

Data-bescherming wordt ondersteund via Volume Shadow Copy Service (VSS) voor consistente snapshots en integratie met back-upoplossingen zoals Microsoft Azure Backup en diverse third-party tools. Opslagencryptie is mogelijk met BitLocker en integratie met externe Key Management Services.

Beveiliging en compliance
Hyper-V is diep geïntegreerd met Microsoft-beveiligingsmechanismen. Authenticatie en autorisatie verlopen via Active Directory en Entra ID (Azure Active Directory). Role Based Access Control (RBAC) kan worden toegepast via Windows, SCVMM en Azure.
Beveiligingsfuncties omvatten Shielded Virtual Machines, Host Guardian Service en encryptie van virtuele disks. Hiermee kunnen gevoelige applicaties worden beschermd tegen ongeautoriseerde toegang, zelfs door beheerders.
Audit logging en monitoring zijn beschikbaar via Windows Event Logs, Windows Admin Center en aanvullende tooling zoals Micros oft Defender for Cloud. Compliance kan worden ondersteund via integratie met Microsoft Purview en security baselines. Sommige van deze functies vereisen connectiviteit met de Microsoft cloud.

4

Beheer en automatisering

Ondersteuning en beheer van containers
Microsoft biedt containerondersteuning via Windows Containers en Kubernetes. Voor moderne omgevingen is de Edge Essentials versie van Azure Kubernetes Service (AKS) de primaire oplossing. Hiermee kunnen containers en virtuele machines naast elkaar worden beheerd binnen één infrastructuur. AKS Edge Essentials is gecertificeerd voor CNCF conformance.

3

De integratie met het onderliggende Hyper-V platform maakt het mogelijk om infrastructuur, network en opslag centraal te beheren, terwijl applicatieteams gebruikmaken van Kubernetes-standaarden.

Lifecycle management
Lifecycle management wordt verzorgd via Windows Update en Cluster-Aware Updating (CAU). Hiermee kunnen hosts en clusters declaratief en rolling worden bijgewerkt met minimale disruptie.

3

Firmware- en driverupdates kunnen worden geïntegreerd via hardwarepartners en Windows Admin Center, waardoor zowel het besturingssysteem als de onderliggende hardware lifecycle beheerd kan worden.

Automatisering en orkestratie
Hyper-V en het bredere Microsoft-platform bieden uitgebreide automatiseringsmogelijkheden via PowerShell en PowerShell Desired State Configuration (DSC). Indien sprake is van een hybride cloud architectuur met Azure Arc en Azure Automation, kunnen ook REST APIs gebruikt worden en is integratie met tools zoals Ansible en Terraform mogelijk.

3

Observability en monitoring
Monitoring van Hyper-V-omgevingen is mogelijk via Windows Admin Center, System Center Operations Manager (SCOM) en Azure Monitor (wanneer een hybride cloud architectuur wordt toegepast). Deze tools bieden inzicht in CPU, geheugen, opslag en netwerkprestaties, met ondersteuning voor alerts en rapportages.

Integratie met third-party monitoringoplossingen zoals Datadog, Grafana en Splunk is beschikbaar via agents en APIs

3

Integratie in bestaande beheersystemen
Microsoft biedt een breed ecosysteem aan integraties. De combinatie met Windows en Azure technologie maakt Hyper-V geschikt voor hybride omgevingen. Third party oplossingen (Veeam, Commvault, NetApp, etc.) bieden uitgebreide ondersteuning.

4

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
Voor organisaties met ervaring met andere virtualisaties platformen, zoals VMware en die al gebruik maken van Windows Server is een overstap naar Hyper-V beheersbaar omdat er conceptueel weinig wijzigingen zijn en de organisatie van de tooling bekend zal zijn. Voor Linux georiënteerde teams kan er extra training nodig zijn.

Met name rondom netwerken heeft Hyper-V beperkingen ten opzichte van de marktleiders en dit vertaalt zich in het gebruik van third party oplossingen die apart beheerd moeten worden, hetgeen impact op de organisatie kan hebben.

TB

Licentie en abonnement
Hyper-V is inbegrepen in Windows Server licenties die beschikbaar zijn als eeuwigdurend gebruiksrecht en aangeschaft worden per core. Afhankelijk van hoe Windows Server gebruikt wordt, zijn eventueel ook nog Client Access Licenses nodig die ook eeuwigdurend zijn. Dit maakt het licentiemodel voorspelbaar, hoewel voor uitgebreide ondersteuning en recht om te upgraden naar de volgende versie Software Assurance vereist is, waarvoor jaarlijks 25-30% van de licentiekosten betaald moeten worden.

4

Overdraagbaarheid van licenties
Indien Software Assurance aangeschaft is, kunnen licenties overgedragen worden naar andere omgevingen.

4

Ondersteuningsmodel en ecosysteem
Microsoft biedt ondersteuning via Software Assurance, Premier/Unified Support en een groot partner-ecosysteem. De beschikbaarheid van kennis in de markt is hoog, mede door de brede adoptie van Windows Server.

5

Migratie en exit
Migratie vanaf VMware kan met VMware conversietools, Microsoft Virtual Machine Converter (MVMC) of via 3rd party tools.
Migratiecomplexiteit hangt af van applicatiespecifieke integraties.
Exit naar andere platformen is mogelijk, maar afhankelijk van gebruikte Microsoft-specifieke integraties.

4

Innovatie
Microsoft investeert sterk in hybrid cloud, Azure integraties, security (Shielded VMs, HGS) en S2D optimalisaties. De innovatie in Hyper-V zelf is relatief beperkt.

4

Omscholing en beschikbaarheid van talent
Er is ruime beschikbaarheid van Microsoft-expertise. Microsoft Learn en certificeringsprogramma's ondersteunen omscholing en verdieping.

5

Autonomie en continuïteit van de leverancier
Windows Server vereist geen verbinding om de licentie te valideren en kan dus blijven draaien wanneer er zich gebeurtenissen voordoen waardoor (langdurig) geen connectiviteit beschikbaar is.
Microsoft is een zeer kapitaalkrachtige leverancier met een lange termijnstrategie op hybride cloud, wat de continuïteit van het platform hoog maakt.

4

Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten zij levert. Dit zou met name invloed hebben op Software Assurance en daarmee op ondersteuning en toekomstige updates.

Kosten (Total Cost of Ownership)
TCO hangt samen met Windows Server licenties en hardware. Voor organisaties met bestaande Microsoft contracten (EA/CSP) kan Hyper-V financieel aantrekkelijk zijn; hybride integraties met Azure kunnen extra kosten meebrengen. Bekende omgeving voor Windows beheerders en realtief makelijk migratie pad

4

Nutanix

Nutanix staat met een marktaandeel van circa 25% op de tweede plaats in de virtualisatiemarkt, op gepaste afstand van VMware. Nutanix biedt zowel een hypervisor als een beheerplatform wat met meerdere hypervisors kan werken en dat maakt het een interessante optie. Nutanix probeert met aantrekkelijke deals marktaandeel af te snoepen van VMware. Net als VMware is Nutanix Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor
Nutanix levert virtualisatie primair via Nutanix Acropolis Hypervisor (AHV). AHV is een enterprise-grade hypervisor die geïntegreerd is in het Nutanix Cloud Platform (NCP) en standaard is inbegrepen zonder aanvullende hypervisorlicentie. Nutanix kan echter ook gebruik maken van VMware ESXi en Microsoft Hyper-V, en zelfs meerdere hypervisors tegelijk aansturen. AHV is gebaseerd op KVM en wordt intensief door Nutanix doorontwikkeld. De hypervisor staat bekend om zijn stabiliteit, geïntegreerd beheer en voorspelbare prestaties in enterprise omgevingen. Hardware assisted virtualisatie (Intel VT x / AMD V, SR IOV) wordt volledig ondersteund.

5

Live migratie (Live Migration), automatische workloadplaatsing en resource optimalisatie worden geleverd via AHV in combinatie met

Nutanix Acropolis Operating System (voor opslag en netwerkvirtualisatie) en Prism (management). Het aantal nodes per cluster hangt af van de hypervisor die gebruikt wordt, waarbij Nutanix tot dat aantal nodes (tusen 32 en 48) getest heeft, maar er geen harde limiet is om meer nodes op te nemen in een cluster. Ook het aantal virtuele machines per cluster heeft geen harde limiet en is gebonden aan de hardwareconfiguratie. Multi clusterbeheer en multi datacenter ondersteuning zijn standaard beschikbaar via Prism Central.
Compatibiliteit met hardware wordt gewaarborgd via de Nutanix Hardware Compatibility List (HCL), die OEM-platforms zoals Dell, Lenovo en HPE omvat. AHV ondersteunt standaard x86-hardware en biedt mogelijkheden voor GPU-passthrough voor grafisch-intensieve workloads. Nutanix ondersteunt momenteel geen Confidential Computing.

Voor gast-OS biedt AHV brede ondersteuning, waaronder Windows, Linux en Unix, met Nutanix Guest Tools voor optimale integratie. Hoewel Nutanix een hoge mate van compatibiliteit biedt voor veel standaardsoftware, dient specifieke software altijd gevalideerd te worden. De integratie met enterprise-applicaties zoals SAP en Oracle is mogelijk mits voldaan wordt aan de hardware- en configuratievereisten.

Opslag en opslagintegratie

Opslag is een kernonderdeel van het Nutanix platform en wordt geleverd via Nutanix AOS (Acropolis OS). AOS vormt een software defined opslaglaag die lokale disks van alle nodes samenvoegt tot één gedistribueerde datastore.
AOS ondersteunt verschillende architecturen:

- Hyperconverged (compute + storage op dezelfde nodes)
- Storage only clusters
- Mixed omgevingen met verschillende node types

Data wordt beschermd door middel van replication factor en/of erasure coding. Performance en beschikbaarheid zijn instelbaar via storage policies per workload. Compressie, deduplicatie en snapshots zijn standaard beschikbaar.
Integratie met externe opslag is mogelijk via iSCSI, NFS en integratie met object storage (bijvoorbeeld S3 compatible oplossingen). Voor disaster recovery en dataprotectie biedt Nutanix Leap, Replication en Snapshots, met ondersteuning voor metro clusters en actieve/actieve scenario's.
Encryptie-at-rest en in transit encryptie worden standaard ondersteund, inclusief integratie met externe Key Management Systems (KMS).

4

(Software Defined) Netwerken

Nutanix biedt software-defined networking via Nutanix Flow, dat geïntegreerd is met AHV en Prism. Flow levert virtuele netwerken, microsegmentatie en gedistribueerde firewallfunctionaliteit zonder afhankelijk te zijn van externe netwerkvirtualisatieplatformen.
De netwerklaag is primair gericht op integratie met bestaande fysieke netwerken; onderliggende switching en routing blijven buiten Nutanix. Binnen het cluster kunnen netwerken centraal beheerd en geautomatiseerd worden. Flow ondersteunt beveiligingsbeleid op VM-niveau, wat het mogelijk maakt om oost-west-verkeer te beveiligen zonder applicatie-afhankelijke configuraties.

3

Voor complexere use-cases kan Nutanix integreren met externe load balancers en netwerkoplossingen. De focus ligt daarbij op eenvoud en geïntegreerd beheer in plaats van een volledig abstracte netwerkfabric over meerdere datacenters heen.Container en VM netwerken kunnen centraal beheerd worden met consistente security policies.

Hybride netwerken worden ondersteund via via VPN-tunnels en service chaining, maar er is geen ingebouwde multi-site overlay abstractie. Integratie met Cisco ACI is beperkt mogelijk via VLANs en handmatige netwerkconfiguratie.

Bedrijfscontinuïteit□

Nutanix biedt hoge beschikbaarheid via automatische herstart van virtuele machines bij node uitval. Virtuele machines en containerapplicaties worden automatisch opnieuw gestart op beschikbare nodes binnen hetzelfde cluster.
Voor disaster recovery biedt Nutanix:

- Asynchrone replicatie met instelbare RPO's
- Metro Availability voor synchrone actieve/actieve configuraties
- Leap runbooks voor georkestreerde failover en failback

Failover tests kunnen non disruptive worden uitgevoerd, wat essentieel is voor compliance en operationele zekerheid.
Een interessante mogelijkheid van Nutanix is Cross Hypervisor Disaster Recovery, hetgeen het mogelijk te maken om noodherstel te doen naar een andere hypervisor, bijvoorbeeld van AHV naar VMware ESXi of andersom.

4

Beveiliging en compliance

Prism ondersteunt integratie met Active Directory en LDAP. Role Based Access Control (RBAC) maakt granulariteit in toegangsbeheer mogelijk. Audit logging en uitgebreide monitoring zijn standaard beschikbaar.

4

Flow microsegmentatie maakt applicatie gerichte beveiligingsmodellen mogelijk zonder afhankelijkheid van netwerk topologie. Encryptie van data, secure boot en platform hardening ondersteunen compliance eisen in gereguleerde omgevingen.

Beheer en automatisering

Ondersteuning en beheer van containers

Nutanix ondersteunt containers via Nutanix Kubernetes Engine (NKE), een CNCF-conforme Kubernetes-distributie die geïntegreerd is met Prism Central. Hiermee kunnen virtuele machines en containers naast elkaar beheerd worden vanuit één beheerlaag, met gedeelde infrastructuur voor compute, storage en netwerk.
NKE ondersteunt lifecycle management van Kubernetes-clusters, inclusief upgrades en schaalvergroting, en integreert met de onderliggende storage- en netwerkdiensten van Nutanix.

4

Lifecycle management

Lifecycle management is een van de sterke punten van Nutanix en wordt geleverd via Lifecycle Manager (LCM). LCM biedt one-click upgrades voor hypervisor, opslag, firmware en hardware-drivers, gebaseerd op een gevalideerde compatibiliteitsmatrix. Dit vermindert operationele complexiteit en downtime aanzienlijk.

5

Automatisering en orkestratie

Nutanix ondersteunt automatisering via:

- REST APIs
- Nutanix Calm (applicatie orkestratie)
- Integratie met Terraform, Ansible en andere 3rd party tools

Nutanix Calm biedt orkestratie van applicaties en infrastructuur via blauwdrukken, inclusief versiebeheer en herhaalbare deployments, waarmee het mogelijk is om uitrol, schalen en levenscyclusbeheer geheel te modelleren voor applicaties.

4

Observability en monitoring
Prism biedt geïntegreerde monitoring en analyse mogelijkheden voor compute, storage en netwerk. Capaciteitsplanning, anomaliedetectie en performance analyse zijn standaardfunctionaliteiten.
Integraties met externe observability platformen zoals Splunk, Datadog en Grafana zijn beschikbaar voor organisaties met bestaande monitoring standaarden.

4

Integratie in bestaande beheersystemen
Nutanix heeft een groeiend ecosysteem met integraties voor backup, security en monitoring. Veel bekende leveranciers (bijvoorbeeld Veeam, Rubrik, Veritas) bieden standaard ondersteuning voor Nutanix.

3

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
Voor organisaties met ervaring met andere virtualisaties platformen, zoals VMware is een overstap naar Nutanix beheersbaar omdat er conceptueel weinig wijzigingen zijn. Dit geldt ook als er behoorlijk wat containerapplicaties zijn. Er is wel omscholing vereist om specifieke functies en concepten van AHV, Prism en AOS te leren kennen.

TB

Licentie en abonnement
Nutanix werkt met een abonnementsmodel per node of per core. De hypervisor (AHV) kent geen afzonderlijke licentiekosten, wat het kostenmodel transparanter maakt. Wanneer gebruik gemaakt wordt van een 3rd party hypervisor, zijn daar wel afzonderlijke licenties voor nodig.

4

Overdraagbaarheid van licenties
Licenties zijn flexibel inzetbaar binnen on premises, edge en ondersteunde cloud omgevingen, afhankelijk van het gekozen Nutanix abonnement.

5

Ondersteuningsmodel en ecosysteem
Nutanix levert support direct op het volledige platform (stack support). Hierdoor is er één aanspreekpunt voor hypervisor, opslag en beheerlaag.
Het ecosysteem groeit snel, met brede ondersteuning door system integrators en managed service providers.

4

Migratie en exit
Nutanix biedt standaard tooling voor migratie vanaf VMware en Microsoft Hyper-V, inclusief VM conversie met minimale downtime middels Cross Hypervisor Disaster Recovery (CHDR). Ook zijn er standaardprocessen om fysieke servers naar Nutanix over te zetten.
Bij een exit kan CHDR mogelijk gebruikt worden voor de migratie van virtuele machines. Alternatief kunnen tools als Veeam gebruikt worden om naar andere platformen te migreren. Migratiecomplexiteit neemt toe naarmate meer Nutanix specifieke diensten zoals Calm (automatisering) en Flow (netwerk) worden gebruikt, omdat de specifieke configuratie daarvan in een ander platform.

5

Innovatie
Nutanix investeert sterk in hybride multi cloud, automatisering en applicatiegerichte infrastructuur. De roadmap richt zich op vereenvoudiging, platform consistente bediening en cloud portabiliteit. Verder investeert Nutanix zoals veel organisaties in AI-functionaliteit en voor het virtualisatieplatform specifiek om AI-applicaties uit te kunnen voeren.

4

Omscholing en beschikbaarheid van talent

Nutanix biedt uitgebreide documentatie, online trainingen en certificeringen. De beschikbaarheid van Nutanix specialisten groeit, mede door VMware klanten die naar alternatieven kijken. Nutanix heeft een geschat marktaandeel van circa 25%, tegenover VMware ruim 40%.

4

Autonomie en continuïteit van de leverancier

Nutanix opereert als zelfstandige leverancier met sterke focus op software. Wanneer gebruik gemaakt wordt van Dark Site licensing functioneert hjet platform volledig onafhankelijk van externe licentievalidatie voor de duur van de licentietermijn. Na de licentietermijn dient een nieuwe licentie in het systeem ingevoerd te worden.

4

Nutanix heeft een marktwaarde van circa 11 miljard USD, hetgeen betekent dat het alleen overgenomen kan worden door kapitaalkrachtige partijen. Nutanix is inmiddels een stabiel bedrijf dat op bescheiden schaal winst maakt (ruim 100 miljoen USD per jaar) al is de winst ten opzichte van de inkomsten stijgende,
Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten zij levert.

Kosten (Total Cost of Ownership)

Nutanix probeert actief marktaandeel te winnen door een aantrekkelijke prijsstrategie als het gaat om licenties. In veel scenario's resulteert het ontbreken van hypervisorlicentiekosten en vereenvoudigd beheer in een lagere of beter voorspelbare softwarekosten ten opzichte van de grote rivaal VMware, met name in middelgrote en grote omgevingen. Kosten voor hardware zijn vergelijkbaar met andere platform en. Het beheer is geoptimaliseerd om zo veel mogelijk geautomatiseerd te doen. Migratie van Vmware naar Nutanix is eenvoudig door goede tooling en conceptueel is Nutanix vergelijkbaar met VMware.

4

OpenNebula

OpenNebula is een open source cloud en virtualisatieplatform dat is ontworpen voor het bouwen en beheren van private, hybrid en edge cloudomgevingen. In tegenstelling tot sterk geïntegreerde HCI platformen positioneert OpenNebula zich als een cloud orchestra tion laag boven bestaande virtualisatie en infrastructuurcomponenten. Het is hierdoor minder een vervanging voor een virtualisatieplatform, maar kan wel als zodanig gebruikt worden door te werken met een KVM-gebaseerde hypervisor. Dit vergt wel extra expertise en is daarom minder kosteneffectief dan.
Omdat het ook gebruikt kan worden met VMware en Microsoft Hyper-V, kan het gebruikt worden om daarvan in stappen weg te migreren en op den duur licentiekosten te besparen.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor

Voor virtualisatie ondersteunt OpenNebula meerdere hypervisors, waaronder KVM (primair en meest gebruikt), VMware ESXi en LXC voor containerapplicaties. KVM vormt in de praktijk de kern van de meeste OpenNebula implementaties en biedt een type 1 hypervisor op basis van Linux kerneltechnologie. OpenNebula abstraheert de onderliggende hypervisor en levert centraal beheer, scheduling en life cycle management van virtuele machines.

4

De schaalbaarheid is gericht op cloud omgevingen met meerdere clusters en datacenters. OpenNebula ondersteunt placement polic ies, resource pools en host aggregaties om applicaties te verdelen over de beschikbare rekenkracht. Live migratie, high availability en resource scheduling zijn beschikbaar, waarbij de exacte mogelijkheden afhankelijk zijn van de gekozen hypervisor en configuratie. Ondersteuning voor gast besturingssystemen volgt grotendeels de mogelijkheden van KVM en de gebruikte Linux distributie.

Opslag en opslagintegratie

OpenNebula levert zelf geen opslagplatform, maar integreert met bestaande opslagsystemen backends. Opslag wordt aangeboden via datastores die gekoppeld zijn aan externe storage oplossingen. Ondersteunde opslagtypen omvatten lokale storage, NFS, iSCSI, Fibre Channel en software defined storageplatformen zoals Ceph.

Het platform ondersteunt meerdere opslag types voor images, system disks en files, waardoor scheiding mogelijk is tussen performance kritische en minder kritische applicaties. Functionaliteit zoals snapshots, cloning en thin provisioning is beschikbaar, maar is in sterke mate afhankelijk van de onderliggende storage technologie. OpenNebula fungeert hierbij als orkestratielaag en biedt geen eigen data services zoals deduplicatie of compressie.

3

Voor databescherming ondersteunt OpenNebula snapshots op VM en disk niveau en integratie met externe backup en replicatieoplossingen. Encryptie van data at rest en in transit is mogelijk via de onderliggende storage en netwerklaag, maar wordt niet native door OpenNebula zelf afgedwongen.

(Software Defined) Netwerken

Netwerkfunctionaliteit binnen OpenNebula wordt geleverd via integratie met Linux netwerktechnologieën en optioneel Software Defined Networking. OpenNebula ondersteunt onder andere Linux bridges, Open vSwitch en VLAN en VXLAN gebaseerde netwerken.
Voor meer geavanceerde use cases biedt OpenNebula ondersteuning voor virtuele netwerken met isolatie, IP address management en security groups. Microsegmentatie en gedistribueerde firewallfunctionaliteit zijn mogelijk, maar vereisen aanvullende configuratie en tooling in de onderliggende netwerkstack.

3

De netwerklaag is sterk afhankelijk van het bestaande fysieke netwerkontwerp. OpenNebula abstraheert het netwerk voor cloudgebruikers, maar neemt geen volledige controle over routing en switching over meerdere datacenters. Integratie met load balancers en externe netwerkdiensten is mogelijk via extensies en API koppelingen.

Bedrijfscontinuïteit

OpenNebula ondersteunt hoge beschikbaarheid voor virtuele machines door middel van monitoring en automatische herstart op alternatieve hosts bij uitval. De effectiviteit en hersteltijd zijn afhankelijk van de gebruikte hypervisor, gedeelde opslag en netwerkconfiguratie.

2

Voor noodherstel biedt OpenNebula geen volledig geïntegreerde end to end oplossing, maar wel mogelijkheden voor replicatie en failover via externe storage en replicatietechnologieën. Orkestratie van herstelprocessen kan worden gerealiseerd via templates en automatisering, maar vereist doorgaans maatwerk en aanvullende tooling.

Beveiliging en compliance

Beveiliging binnen OpenNebula is gebaseerd op een combinatie van platformfunctionaliteit en integratie met externe systemen. Het platform ondersteunt Role Based Access Control (RBAC), multi tenancy en resource isolatie via virtual datacenters.

3

Integratie met directorydiensten zoals LDAP en Active Directory is mogelijk voor authenticatie en autorisatie. Audit logging, quota beheer en policy based resource toewijzing ondersteunen compliance doelstellingen. Hardening en patching van de infrastructuur vallen grotendeels onder de verantwoordelijkheid van de beheerorganisatie en de gebruikte Linux distributies.

Beheer en automatisering

Ondersteuning en beheer van containers

OpenNebula ondersteunt containers via LXC en integratie met Kubernetes omgevingen. Kubernetes wordt niet als volledig beheerde dienst geleverd, maar kan wel worden uitgerold en beheerd via OpenNebula templates en automatisering op verschillende manieren, waaronder integratie met Rancher. Een nieuwe versie die de integratie moet verbeteren is in ontwikkeling.

3

Deze benadering maakt het mogelijk om virtuele machines en container platformen binnen één cloudomgeving te combineren, maar vereist meer handmatige inrichting dan platforms met diep geïntegreerde Kubernetes services.

Lifecycle management

Netwerkfunctionaliteit binnen OpenNebula wordt geleverd via integratie met Linux netwerktechnologieën en optioneel Software Defined Networking. OpenNebula ondersteunt onder andere Linux bridges, Open vSwitch en VLAN en VXLAN gebaseerde netwerken.
Voor meer geavanceerde use cases biedt OpenNebula ondersteuning voor virtuele netwerken met isolatie, IP address management en security groups. Microsegmentatie en gedistribueerde firewallfunctionaliteit zijn mogelijk, maar vereisen aanvullende configuratie en tooling in de onderliggende netwerkstack.

2

De netwerklaag is sterk afhankelijk van het bestaande fysieke netwerkontwerp. OpenNebula abstraheert het netwerk voor cloudgebruikers, maar neemt geen volledige controle over routing en switching over meerdere datacenters. Integratie met load balancers en externe netwerkdiensten is mogelijk via extensies en API koppelingen.

Automatisering en orkestratie

OpenNebula biedt uitgebreide automatiseringsmogelijkheden via REST APIs, CLI tools en service templates. Applicaties en infrastructuur kunnen worden gedefinieerd als herhaalbare templates met versiebeheer.

3

Integratie met externe automatiseringstools zoals Ansible en Terraform is mogelijk, waarbij OpenNebula fungeert als orchestrator voor rekenkracht, netwerk en opslag.

Observability en monitoring

Monitoring binnen OpenNebula omvat inzicht in resource gebruik, beschikbaarheid en capaciteit. Basisstatistieken zijn beschikbaar via de webinterface en APIs. Voor geavanceerde observability is integratie met externe monitoring en loggingplatformen gebruikelijk.

2

Integratie in bestaande beheersystemen

OpenNebula is sterk gericht op integratie. Via open APIs en een modulair ontwerp kan het platform worden gekoppeld aan bestaande backup , monitoring , identity en billing systemen. Het ecosysteem is kleiner en minder gestandaardiseerd dan dat van commerciële platforms, maar biedt veel vrijheid voor maatwerk.

3

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

OpenNebula vraagt doorgaans meer Linux en cloud expertise binnen de organisatie. Daarnaast is OpenNebula nog een relatief onvolwassen technologie waar veel andere tooling omheen nodig is en de organisatie veel verantwoordelijkheid moet dragen voor de operatie. Dat is

TB

zeker voor kleinere organisaties moeilijk om op te bouwen. Daartegenover staat een hoge mate van flexibiliteit en controle over architectuur en processen, hetgeen in een grotere en volwassen IT-organisatie voordelen op kan leveren.
OpenNebula kan in eerste instantie als extra beheerlaag bovenop VMware ingezet worden om vervolgens richting KVM te bewegen. Dit vergt een transitie van de organisatie en expertise.

Licentie en abonnement
OpenNebula is beschikbaar als open source software onder een Apache 2.0 licentie en is beschikbaar op GitHub. Daarnaast wordt een commercieel abonnement aangeboden voor enterprise ondersteuning en aanvullende functionaliteit. Dit model reduceert licentiekosten, maar verlegt de focus naar operationele inzet en expertise.

5

Overdraagbaarheid van licenties
Door het open source karakter zijn er geen klassieke licentiebeperkingen. Het platform kan vrij ingezet worden in on premises, edge en hybride cloudomgevingen.

5

Ondersteuningsmodel en ecosysteem
Commerciële ondersteuning wordt geleverd door de OpenNebula leverancier en partners. Het ecosysteem is een stuk beperkter dan dat van bijvoorbeeld VMware of Nutanix en leunt sterk op community gedreven ontwikkeling. De OpenNebula organisatie zelf is niet erg groot, wat negatieve invloed kan hebben op de ondersteuning.

2

Migratie en exit
Migratie naar OpenNebula vereist doorgaans conversie van virtuele machines en herontwerp van netwerk en storage integraties.
Exit is relatief eenvoudig doordat applicaties draaien op standaard hypervisors en open technologieën. Hierbij moet aangemerkt worden dat dit wel afhangt van hoe de onderliggende hypervisor is ingericht, maar OpenNebula kan hierbij zelf als migratietool gebruikt worden.

4

Innovatie
OpenNebula richt innovatie primair op cloud orchestratie, edge use cases en integratie met open source technologieën. De ontwikkelsnelheid is stabiel, maar minder commercieel gedreven dan bij grote leveranciers.

2

Omscholing en beschikbaarheid van talent
Expertise is vooral te vinden bij organisaties met sterke Linux , KVM en open source achtergrond. De beschikbaarheid van gespecialiseerde OpenNebula kennis is beperkter dan bij commerciële platformen.

3

Autonomie en continuïteit van de leverancier
OpenNebula is een organisatie die verdeeld is over de VS en Spanje, met ontwikkelaars in andere Europese landen. Er zijn circa 170 ontwikkelaars die bijdragen aan het open source project, hetgeen een reflectie is van hoe actief er ontwikkeld wordt en de grootte van de organisatie.

Het open source karakter biedt een hoge mate van autonomie en beperkt leveranciersafhankelijkheid. Continuïteit is gekoppeld aan de actieve community en commerciële ondersteuning, maar er is geen technische lock in, waardoor er weinig risico is t.a.v. autonomie en continuïteit.

4

Kosten (Total Cost of Ownership)

Hoewel de kosten voor licentie en ondersteuning laag zijn, moet een organisatie goed in staat zijn om zelf problemen op te lossen. Hierdoor kunnen operationele kosten hoger uitvallen door complexiteit en benodigde expertise. Voor organisaties met bestaande open source kennis kan OpenNebula een kosteneffectieve oplossing zijn. Doordat OpenNebula een ander concept gebruikt kan een migratie complex zijn.

3

Oracle Linux Virtualization Manager

Oracle Linux Virtualization Manager (OLVM) is een server virtualisatiebeheerplatform dat is ontworpen om een Oracle Linux Kernel-gebaseerde Virtual Machine (KVM)-omgeving te configureren, monitoren en beheren.
Oracle is Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Noot: Oracle OLVM is wat anders dan Oracle OVM, wat niet meer ondersteund wordt. Zie Appendix D – Andere alternatieven voor meer informatie.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor

Virtualisatie van hardware binnen Oracle Linux Virtualization Manager wordt geleverd door Oracle Linux KVM, een hypervisor die onderdeel is van de Linux kernel en gebaseerd is op het open source KVM project. Oracle positioneert OLVM als de strategische opvolger van Oracle VM en als primaire virtualisatielaag voor on premises Oracle omgevingen.

KVM is een bewezen type 1 hypervisor die gebruikmaakt van hardware assisted virtualisatie (Intel VT x en AMD V). In combinatie met Oracle Linux en de Unbreakable Enterprise Kernel (UEK) biedt OLVM een stabiel en performant platform voor bedrijfskritische workloads, met name Oracle Database, Oracle RAC en middleware toepassingen. De hypervisor is generiek van aard, maar Oracle optimaliseert het platform nadrukkelijk voor gebruik in combinatie met Oracle software.

4

OLVM ondersteunt live migratie van virtuele machines tussen hosts binnen een cluster, waardoor onderhoud kan plaatsvinden zonder downtime. Resource toewijzing voor CPU en geheugen kan dynamisch aangepast worden, waarbij scheduling plaatsvindt op clusterniveau. De schaalbaarheid is geschikt voor middelgrote tot grote omgevingen, waarbij meerdere clusters en datacenters beheerd kunnen worden vanuit één centrale OLVM engine.

Ondersteuning voor gastbesturingssystemen is het meest uitgebreid voor Oracle Linux en andere RHEL compatibele Linux distributies. Microsoft Windows wordt ondersteund via VirtIO drivers. De focus ligt duidelijk op Linux gebaseerde workloads; certificering en ondersteuning van overige besturingssystemen is beperkter dan bij marktleidende hypervisors.

Opslag en opslagintegratie

Opslag binnen OLVM wordt aangeboden via het storage domain model, waarbij gedeelde opslag centraal beschikbaar wordt gesteld aan alle hosts binnen een cluster. Dit maakt live migratie, hoge beschikbaarheid en gecentraliseerd beheer van virtuele disks mogelijk .
OLVM ondersteunt verschillende typen enterprise opslag, waaronder NFS, iSCSI en Fibre Channel. Lokale opslag kan worden gebruikt voor specifieke scenario's, maar wordt niet aanbevolen voor productieomgevingen waarin hoge beschikbaarheid vereist is. Opslagdomeinen worden gebruikt voor het opslaan van virtuele machine disks, templates en ISO bestanden.

3

Databeveiliging en beschikbaarheid zijn grotendeels afhankelijk van de onderliggende opslagoplossing. OLVM ondersteunt snapshots op VM niveau, maar deze zijn primair bedoeld voor kortdurend gebruik en niet als vervanging voor structurele backup of hersteloplossingen. Voor disaster recovery en dataprotectie wordt doorgaans gebruikgemaakt van storage gebaseerde replicatie of backupsoftware binnen de virtuele machines zelf.

TB

In tegenstelling tot sommige hyperconverged platforms beschikt OLVM niet over een native software defined storage laag vergelijkbaar met vSAN. Optimalisatie van opslagprestaties en redundantie ligt daarom grotendeels buiten het virtualisatieplatform.

(Software Defined) Netwerken

Voor netwerkfunctionaliteit biedt OLVM logische netwerken bovenop de fysieke infrastructuur. Virtuele machines worden verbonden met deze logische netwerken via virtuele NIC profielen, waarbij VLAN segmentatie en Quality of Service toegepast kunnen worden.
OLVM ondersteunt NIC bonding voor redundantie en performance, zowel in active active als active passive configuraties.
Netwerkconfiguratie vindt plaats op host en clusterniveau en wordt centraal beheerd via de OLVM engine.

3

De netwerkfunctionaliteit is gericht op stabiliteit en basissegmentatie, maar blijft beperkt tot traditionele L2/L3 concepten. Geavanceerde software defined networking functionaliteit zoals overlay netwerken, microsegmentatie, gedistribueerde firewalls en zero trust architecturen is niet standaard onderdeel van het platform. Voor dergelijke functionaliteit is integratie met externe netwerk en securityoplossingen noodzakelijk.

Bedrijfscontinuïteit

OLVM biedt ondersteuning voor hoge beschikbaarheid door middel van cluster gebaseerde failover. Wanneer een fysieke host uitvalt, worden virtuele machines automatisch opnieuw gestart op andere hosts binnen hetzelfde cluster. Dit mechanisme is gebaseerd op herstart en niet op continue beschikbaarheid; korte downtime is daarbij onvermijdelijk.
Live migratie maakt het mogelijk om virtuele machines proactief te verplaatsen voor onderhoud of loadbalancing. Resource scheduling zorgt ervoor dat workloads evenwichtig over het cluster verdeeld worden.

3

Voor noodherstel biedt OLVM geen volledig geïntegreerde orkestratieoplossing. Herstel bij uitval van een datacenter is afhankelijk van externe replicatie, opslagtechnologie en handmatige of semi geautomatiseerde procedures. Het testen en orkestreren van noodherstel scenario's vereist aanvullende tooling of maatwerkprocessen.

Beveiliging en compliance

Beveiliging binnen OLVM is grotendeels gebaseerd op standaard Linux en KVM mechanismen. Authenticatie en autorisatie kunnen geïntegreerd worden met directorydiensten zoals LDAP en Active Directory. Role Based Access Control maakt het mogelijk om beheertaken te scheiden en gebruikers verschillende rechten toe te kennen.

Encryptie van data at rest en data in transit wordt niet centraal door OLVM afgedwongen, maar is afhankelijk van de gebruikte opslagoplossing, het gastbesturingssysteem en de applicatieconfiguratie. Audit logging en event logging zijn beschikbaar via de OLVM engine en kunnen worden geëxporteerd naar externe monitoring of SIEM oplossingen.
Voor compliance doeleinden wordt OLVM vaak gecombineerd met Oracle Enterprise Manager, met name in omgevingen waar Oracle Database een centrale rol speelt.

3

Beheer en automatisering

Ondersteuning en beheer van containers

OLVM is primair gericht op het beheren van virtuele machines en biedt geen geïntegreerde ondersteuning voor containers of Kubernetes. Oracle positioneert containerplatformen los van OLVM, meestal op Oracle Linux (bare metal of virtueel). Hierdoor worden containers en virtuele machines niet geïntegreerd beheerd binnen één platform.

1

Lifecycle management

Lifecycle management binnen OLVM is functioneel maar beperkt. Updates van hypervisorhosts worden uitgevoerd via de Oracle Linux package repositories, terwijl upgrades van de OLVM engine een afzonderlijk proces vormen. Er is geen declaratief model waarbij een gewenste eindstatus van hosts centraal wordt afgedwongen.

Rolling upgrades zijn mogelijk, maar vereisen zorgvuldige planning om downtime en risico's te beperken. Firmware en hardware updates vallen buiten de scope van OLVM en moeten via externe tooling of leveranciersprocessen worden uitgevoerd.

2

Automatisering en orkestratie

OLVM biedt automatiseringsmogelijkheden via een REST API, command line interfaces en integratie met Ansible. Hiermee kunnen beheertaken gescript en geautomatiseerd worden, bijvoorbeeld voor provisioning van virtuele machines en basisconfiguratie

De mate van automatisering is voldoende voor standaard use cases, maar minder uitgebreid en minder geïntegreerd dan bij platforms die beschikken over een volledige orchestratie en workflow suite. Er is geen grafische workflow designer of uitgebreide bibliotheek met kant en klare automatiseringsflows.

2

Observability en monitoring

Monitoring binnen OLVM vindt plaats via ingebouwde dashboards, event logging en geïntegreerde Grafana dashboards. Deze bieden inzicht in resourcegebruik van CPU, geheugen, opslag en netwerk op host en VM niveau.

Voor diepgaande observability en correlatie met applicatie performance zijn externe monitoringtools nodig. In Oracle gerichte omgevingen wordt hiervoor vaak Oracle Enterprise Manager ingezet, terwijl generieke monitoringoplossingen eveneens gebruikt kunnen worden.

3

Integratie in bestaande beheersystemen

Het ecosysteem rondom OLVM is beperkter dan dat van marktleiders, maar sluit goed aan op Oracle gerichte beheer en monitoringtools. Integratie met niet Oracle tooling is mogelijk via standaarden en APIs, maar vereist vaker maatwerk en aanvullende configuratie.

2

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

De impact van OLVM op de organisatie is sterk afhankelijk van de bestaande IT architectuur. Voor organisaties met een sterke focus op Oracle software en Linux kan OLVM goed aansluiten bij bestaande kennis en processen. Voor heterogene omgevingen met meerdere platformen en cloud native ambities is de impact groter, doordat aanvullende tooling en expertise nodig zijn. Dit komt deels ook omdat OLVM relatief beperkt is qua functionaliteit.

TB

Licentie en abonnement
OLVM zelf is licentievrij. Kosten worden vooral bepaald door Oracle Linux supportabonnementen, operationele inzet en in veel gevallen Oracle Database licenties. Een belangrijk kenmerk van Oracle Linux KVM is dat het, mits correct geconfigureerd, door Oracle wordt erkend als hard partitioning technologie. Dit maakt het mogelijk om Oracle Database licenties te beperken tot toegewezen CPU cores, wat een significant kostenvoordeel kan opleveren ten opzichte van soft partitioning platformen.

3

Overdraagbaarheid van licenties
OLVM zelf is licentievrij en daardoor eenvoudig te verplaatsen naar een andere omgeving. Voor de infrastructuur zijn Oracle Linux licenties nodig waarvoor license mobility onderdeel is van het licentiemodel, hetgeen verplaatsen naar een andere omgeving mogelijk maakt.

4

Ondersteuningsmodel en ecosysteem
Oracle biedt enterprise support op OLVM als strategisch platform. Het ecosysteem is kleiner dan dat van de marktleiders, maar stabiel binnen Oracle klanten en partners die gespecialiseerd zijn in Linux en Oracle technologie.

3

Migratie en exit
Migratie naar OLVM is met name relevant voor bestaande Oracle VM omgevingen. Migratie naar OLVM vanuit andere virtualisatieplatformen is mogelijk, maar vereist herontwerp van netwerk , opslag en automatiseringsconcepten. Dit geldt ook voor een exit uit OLVM. Voor een exit zit de complexiteit verder in het verlaten van Oracle specifieke optimalisaties.

2

Innovatie
OLVM profiteert van continue innovatie binnen de Linux kernel, KVM en het oVirt project. Oracle investeert actief in dit platform als strategische virtualisatielaag, waarbij verbeteringen geleidelijk worden doorgevoerd in nieuwe releases.

3

Omscholing en beschikbaarheid van talent
Kennis van OLVM bevindt zich voornamelijk bij Linux en Oracle specialisten. De beschikbaarheid van expertise is beperkter dan bij marktleiders, maar de onderliggende technologie is gebaseerd op open source KVM, waardoor omscholing relatief goed mogelijk is. Doordat het virtualisatieplatform beperkt is in functie, dient wel allerlei kennis opgedaan te worden van andere software.

3

Autonomie en continuïteit van de leverancier
Oracle is een financieel stabiele leverancier met een duidelijke strategische keuze voor OLVM als opvolger van Oracle VM. De continuïteit van het platform is daarmee hoger dan bij Oracle VM, al blijft de afhankelijkheid van Oracle support en beleidskeuzes aanwezig.
Oracle is een zeer kapitaalkrachtige leverancier met een lange termijnstrategie op private cloud, wat de continuïteit van het platform hoog maakt.

Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten zij levert. Dit zou met name invloed hebben op ondersteuning en toekomstige updates, aangezien er geen connectiviteit nodig is om het platform te draaien.

3

Kosten (Total Cost of Ownership)
De totale kosten hangen sterk samen met het gebruik van Oracle software. OLVM biedt voordelen door het ontbreken van hypervisorlicenties, maar operationele kosten kunnen hoger uitvallen door beperktere automatisering en integratie vergeleken met marktleidende platforms. Bij migraties moet er nog veel handmatig werk worden verricht. Goede Linux kennis is een vereiste.

3

Proxmox

Proxmox Virtual Environment (Proxmox VE) is een open-source virtualisatieplatform dat populair is vanwege zijn kostenefficiëntie, flexibiliteit en gebruiksvriendelijke beheerinterface. Het combineert KVM (Kernel-based Virtual Machine) voor volledige virtualisatie en LXC (Linux Containers) voor containers in één geïntegreerde oplossing, al werkt deze anders dan Kubernetes.
Wat Proxmox aantrekkelijk maakt, is de combinatie van krachtige functies zoals hoge beschibaarheid, live migratie, en gedistribueerde opslag, zonder dure licentiekosten. Daarnaast biedt het een actieve community, regelmatige updates en brede hardwarecompatibiliteit, waardoor het een populair alternatief is voor commerciële hypervisors.

Proxmox is een betrekkelijk klein bedrijf en vooralsnog vooral gericht op kleinere organisaties, omdat het bedrijf betrekkelijk klein is en daardoor moeilijk grote organisaties kan ondersteunen. Door de populariteit is dit wel aan het veranderen.

Kernfuncties en kenmerken van het platform

Virtualisatie/hypervisor
Virtualisatie van hardware door een hypervisor wordt door Proxmox geleverd via Proxmox VE wat virtualisatie verzorgt via het open source KVM (Kernel-based Virtual Machine) wat onderdeel uitmaakt van Linux. Dit vormt de kern van alle mogelijkheden die Proxmox biedt en maakt het geschikt voor zowel kleine omgevingen als grotere clusters.

Proxmox VE staat bekend om zijn stabiliteit en flexibiliteit, mede dankzij de Linux-gebaseerde architectuur. Het platform ondersteunt hardware-assisted virtualisatie (Intel VT-x, AMD-V) en biedt functies zoals live migration, waardoor workloads efficiënt en zonder downtime kunnen worden verplaatst, en resource oversubscription, waardoor flexibel omgegaan kan worden met beschikbare capaciteit.
Schaalbaarheid wordt bereikt via clustering: meerdere nodes kunnen eenvoudig worden toegevoegd en centraal beheerd via de geïntegreerde webinterface. Het aantal nodes per cluster is maximaal 32. Proxmox Datacenter Manager om meerdere clusters tegelijk te kunnen beheren via een enkele interface is nog in ontwikkeling en daardoor nog geen volwaardig alternatief voor de oplossingen van de marktleiders, zoals VMware vCenter

4

Compatibiliteit met hardware is breed, omdat Proxmox draait op standaard x86-hardware zonder vendor lock-in. Voor geavanceerde functies zoals PCI passthrough is ondersteuning voor VT-d/AMD-d vereist. GPU-passthrough wordt ondersteund voor grafisch-intensieve toepassingen. Tevens ondersteunt Proxmox de Confidential Computing technologien AMD SEV-SNP en Intel TDX.
Doordat Proxmox gebruik maakt van KVM, geldt dat Proxmox compatibel is met alle gast operating systemen die compatibel zijn met KVM, waaronder Windows, Linux en BSD. Voor optimale performance op Windows-VM's zijn VirtIO-drivers beschikbaar. Welke gast operating systemen worden ondersteund wanneer klanten met een onderhoudscontract ondersteuning vragen is niet duidelijk.
Wat betreft compatibiliteit met specifieke software is Proxmox zeer geschikt voor open-source stacks en kan het integreren met Kubernetes via externe tooling. Voor enterprise-applicaties zoals SAP of Oracle is er geen officiële certificering, waardoor ondersteuning door deze organisatie bij een probleem mogelijk niet gegeven wordt.

Opslag en opslagintegratie
Opslag is een kernonderdeel van Proxmox VE en wordt flexibel ingevuld. Het platform ondersteunt zowel lokale opslag als gedeelde opslag via verschillende technologieën. Daarmee kan Proxmox zowel als klassiek virtualisatieplatform als HCI achtige oplossing worden ingezet.

4

Proxmox VE ondersteunt geïntegreerde software defined storage via Ceph. Met Ceph kunnen lokale disks van meerdere nodes worden samengevoegd tot één gedistribueerde storage laag, met automatische replicatie en fouttolerantie op schijf en node niveau. Ceph

ondersteunt verschillende disktypes (NVMe, SSD, HDD) en biedt block en file opslag.

Naast Ceph ondersteunt Proxmox integratie met externe opslagoplossingen via NFS, iSCSI, Fibre Channel en ZFS gebaseerde opslag. ZFS wordt vaak gebruikt voor lokale opslag en biedt geavanceerde functies zoals snapshots, checksumming en replicatie.

Data bescherming kan worden gerealiseerd via snapshots, back ups en replicatie. Proxmox biedt native back upfunctionaliteit en ondersteuning voor integratie met Proxmox Backup Server. Encryptie van data at rest en data in transit is mogelijk, afhankelijk van gekozen opslagoplossing en configuratie, maar vereist bewuste inrichting door de organisatie.

(Software Defined) Netwerken

Netwerkfunctionaliteit in Proxmox VE is gebaseerd op standaard Linux netwerkcomponenten. Virtuele bridges, VLAN tagging en bonding zijn native beschikbaar en worden centraal beheerd via de Proxmox interface.
Voor meer geavanceerde netwerkfunctionaliteit, zoals microsegmentatie, overlay netwerken of multi tenant SDN scenario's, biedt Proxmox geen geïntegreerde enterprise SDN laag. Dergelijke functionaliteit moet worden ingevuld met externe netwerkoplossingen of aanvullende Linux netwerkconfiguraties.

2

Deze aanpak biedt maximale flexibiliteit en transparantie, maar vraagt diepere netwerkkennis en biedt minder out of the box automatisering dan gespecialiseerde SDN oplossingen.

Bedrijfscontinuïteit

Proxmox VE ondersteunt hoge beschikbaarheid via cluster functionaliteit en HA groepen. Bij uitval van een node kunnen virtuele machines automatisch opnieuw worden gestart op andere nodes binnen het cluster, mits gedeelde opslag beschikbaar is.
Live migratie van virtuele machines is standaard beschikbaar, zowel met als zonder gedeelde opslag. Voor omgevingen met Ceph of gedeelde SAN opslag is live migratie doorgaans transparant voor workloads.

3

Noodherstel op site niveau is niet als volledig georkestreerde oplossing geïntegreerd. Site overstijgend noodherstel vereist handmatige orkestratie of aanvullende tooling, omdat Proxmox standaard geen geautomatiseerde multi site failover biedt. Replicatie en back up kunnen worden ingezet om herstel mogelijk te maken, maar het ontwerpen van DR scenario's vereist maatwerk en aanvullende tooling. RPO en RTO zijn daardoor sterk afhankelijk van architectuurkeuzes en operationele processen.

Beveiliging en compliance

Beveiliging binnen Proxmox VE is gebaseerd op Linux securitymechanismen en role based access control binnen het platform. Authenticatie kan lokaal plaatsvinden of via integratie met externe directory diensten zoals LDAP of Active Directory.
RBAC binnen Proxmox biedt basisrolmodellen voor cluster en datastorebeheer, maar is minder fijnmazig dan bij uitgebreide private cloud suites. Encryptie van data at rest en data in transit is beschikbaar, maar vereist expliciete configuratie van opslag, netwerk en back upoplossingen.

2

Audit logging en monitoring zijn aanwezig, maar compliance rapportage en policy afdwanging worden doorgaans ingevuld met externe security en monitoringtools.
Compliance en hardening zijn grotendeels afhankelijk van Linux standaarden en best practices. Proxmox biedt audit logging, maar minder uitgebreide compliance dashboards dan commerciële suites.

Beheer en automatisering

Ondersteuning en beheer van containers

Proxmox VE ondersteunt containers via LXC en biedt hiermee native OS level containerfunctionaliteit binnen hetzelfde platform als virtuele machines. Deze containers zijn lichtgewicht en geschikt voor infrastructuur en applicatietaken.

2

Een geïntegreerde Kubernetes distributie maakt geen standaard onderdeel uit van het platform. Kubernetes kan wel bovenop Proxmox worden uitgerold, maar wordt niet centraal beheerd vanuit de Proxmox control plane. Hierdoor is de integratie tussen VM en containerbeheer beperkt.

Lifecycle management

Lifecycle management binnen Proxmox VE is grotendeels handmatig of semi geautomatiseerd. Updates van hosts en clustercomponenten worden uitgevoerd via package management en Proxmox tools, met ondersteuning voor rolling updates.
In tegenstelling tot declaratieve lifecycle oplossingen vereist dit goede operationele discipline en documentatie om consistentie tussen nodes te waarborgen.

3

Updates voor hypervisor, beheerlaag en clustercomponenten worden geleverd via het Proxmox repository model en kunnen met de standaard apt-get tooling geïnstalleerd worden. Enterprise repositories bieden getest patchmanagement. Er is geen vaste patch- of update-cyclus. Er is een publieke bug tracker waar bugs gemeld kunnen worden en verzoeken om bepaalde functies te ontwikkelen gedaan kunnen worden. Omdat Proxmox open source is, kan iedereen aanpassingen doen indien er fouten optreden, maar alleen met een onderhoudscontract met Proxmox hebben gebruikers zekerheid dat de wijzigingen getest zijn.
Firmware beheer is niet geïntegreerd; dat blijft afhankelijk van hardwareleveranciers.

Automatisering en orkestratie

Proxmox VE biedt een REST API en command line tools waarmee automatisering mogelijk is. Integratie met tools zoals Ansible en Terraform is beschikbaar, maar minder diepgaand gestandaardiseerd dan bij grote commerciële platformen.
Automatisering richt zich vooral op infrastructuuracties en VM beheer. Geavanceerde orkestratie scenario's vereisen maatwerk of aanvullende tooling.

2

Orchestratie voor multi tier applicaties moet via externe tooling plaatsvinden (bijvoorbeeld Ansible of Kubernetes on top).

Observability en monitoring

Monitoring in Proxmox VE biedt inzicht in CPU , geheugen , opslag en netwerkgebruik per node en per virtuele machine. Deze basisfunctionaliteit is geschikt voor operationeel beheer en troubleshooting.

3

Voor geavanceerde observability, capaciteitsplanning en correlatie over meerdere lagen heen zijn externe monitoring en loggingoplossingen nodig. Integraties met externe monitoringplatformen zoals Prometheus, Grafana en Zabbix zijn eenvoudig te realiseren.

Integratie in bestaande beheersystemen

Proxmox VE integreert via open standaarden en APIs met externe tools. Er is geen uitgebreid gecertificeerd ecosysteem vergelijkbaar zoals bij de commerciële leveranciers, maar wel brede compatibiliteit met open source en generieke enterprise tools. Omdat Proxmox open source is, bestaat een breed ecosysteem aan community en commerciële integraties. Backup, monitoring, provisioning en security oplossingen van

3

derden ondersteunen Proxmox steeds breder, maar certificering ontbreekt doorgaans.
De mate van integratie hangt sterk af van eigen engineering en operationele keuzes

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
De impact op de organisatie hangt af van de bestaande kennis van Linux gebaseerde omgevingen. Voor teams met Linux ervaring is de adoptie eenvoudiger dan teams die uit een Windows ecosysteem komen. Voor teams die uit een VMware of Nutanix omgeving komen vraagt adoptie gewenning aan KVM, Linux netwerken en ZFS/Ceph concepten.

TB

De adoptie van open source vergt verder dat een organisatie beter ingericht is op zelf oplossingen zoeken en met de community te werken om tot oplossingen te komen. Een onderhoudscontract kan hier weliswaar bij helpen, maar de ondersteuning en documentatie zijn minder verfijnd dan bij commerciële oplossingen.

Licentie en abonnement
Proxmox VE is open-source en vrij te gebruiken. Optionele abonnementen zijn beschikbaar voor toegang tot enterprise-repositories en commerciële ondersteuning. Licentiekosten zijn hierdoor aanzienlijk lager dan bij commerciële virtualisatieplatformen. Proxmox biedt betaalde ondersteuning per node.

5

Overdraagbaarheid van licenties
Licenties zijn niet van toepassing zoals bij commerciële software; Proxmox kan vrij worden ingezet op elke ondersteunde hardware.

5

Ondersteuningsmodel en ecosysteem
Ondersteuning wordt geleverd via community ondersteuning of via betaalde Proxmox abonnementen. Het commerciële ecosysteem is kleiner dan bij marktleiders, maar de community is actief en technisch volwassen. Het ecosysteem groeit snel, maar is significant kleiner dan dat van VMware of Nutanix. Communities zijn zeer actief en veel oplossingen zijn vrij beschikbaar. Volgens Proxmox zelf gebruiken ca. 575 organisaties in 142 landen de software, maar aangezien een licentie niet vereist is kan dit aantal meer zijn en zijn er veel hobbyisten die Proxmox gebruiken.

4

De kwaliteit van ondersteuning is sterk afhankelijk van eigen expertise en gekozen supportniveau.

Migratie en exit
Migratie naar Proxmox VE kan plaatsvinden met behulp van conversietools en migratie scripts. Migratie vanaf VMware kan via conversietools zoals virt v2v of via handmatige migraties. Migraties zijn doorgaans mogelijk, maar vereisen planning en validatie. Containers kunnen eenvoudig worden gemigreerd via LXC standaarden, gebruikers van Kubernetes zullen echt eerst een Kubernetes distributie moeten uitrollen op de omgeving. Migratiecomplexiteit neemt toe bij Ceph of ZFS specifieke configuraties.

4

Aangezien Proxmox open source is, is een exit vanwege licentieproblematiek of geopolitieke verandering geen voor de hand liggend scenario. Een exit kan van toepassing zijn als Proxmox aan populariteit verliest, de ontwikkeling van nieuwe mogelijkheden stokt en/of overgenomen wordt door een commerciële partij. Een exit naar andere KVM gebaseerde platformen is relatief eenvoudig. Migratie naar niet KVM platformen vraagt aanvullende tooling en herinrichting.

Innovatie

Innovatie binnen Proxmox richt zich op stabiliteit, verbetering van bestaande functionaliteit en uitbreiding van open source integraties, zoals Ceph en ZFS. De roadmap is pragmatisch en minder gericht op snelle introductie van cloud native features. De Proxmox organisatie is niet groot, waardoor de snelheid van innovatie minder is dan bij commerciële partijen.

3

Omscholing en beschikbaarheid van talent

Linux en KVM kennis is breed beschikbaar in de markt. Specifieke Proxmox kennis is minder algemeen, maar relatief snel op te bouwen voor ervaren Linux beheerders. Beschikbaarheid van Proxmox specialisten groeit, vooral in organisaties die open source strategieën hanteren. Training is beschikbaar via documentatie, community en commerciële partners.

4

Autonomie en continuïteit van de leverancier

Proxmox is volledig open source en kan dus zonder leverancier uitgevoerd worden. Ook voor ondersteuning is geen licentievalidatie vereist, waardoor er in principe geen beperking zijn op het gebruik.

4

Proxmox is een kleine organisatie en is daardoor een makkelijke prooi voor overname door een kapitaalkrachtige partij. Echter, omdat Proxmox open source is, kan een nieuwe partij in dat geval de rol van Proxmox overnemen indien nodig. De overname van bijvoorbeeld Red Hat heeft betrekkelijk weinig invloed gehad op de rol die het bedrijf vervult en voor Proxmox kan in een dergelijke situatie hetzelfde gelden.

Kosten (Total Cost of Ownership)

De kosten voor Proxmox bestaan primair uit hardware, storage en optionele support. Voor grotere Ceph clusters kunnen kosten stijgen door hardware eisen (RAM, NVMe). Waar de totale kosten afwijken van commerciële opties is de manier waarop expertise voor ondersteuning in de organisatie ingebed worden. Doordat de documentatie en ondersteuning minder gestroomlijnd is, vereist Proxmox deels meer seniore mensen die in staat zijn om problemen met open source op te sporen.

4

Rancher Prime

Rancher is een open source platform voor het beheren van multu-cluster Kubernetes omgevingen en gebouwd rondom de open source componenten van de Cloud Native Computing Foundation (CNCF). Rancher Prime is een enterprise variant die ondersteund wordt door Suse met extra opties voor onder andere beveiliging en compliance. Rancher wordt standaard gecombineerd met de RKE2 Kubernetes distributie. In tegenstelling tot klassieke hypervisor-virtualisatie richt Rancher zich primair op container applicaties, maar kunnen virtuele machines beheerd worden via KubeVirt. Het platform abstraheert infrastructuur via Kubernetes en maakt applicatie-implementatie onafhankelijk van de onderliggende hardware of cloud.

Rancher is geheel open source onder een Apache licentie. Rancher Prime bevat ook enkele leverancier eigen componenten van Suse, en wordt daarom niet beschouwd als volledig open-source.

Suse is een multinationaal bedrijf met het hoofdkantoor in Luxemburg en het grootste deel van de operatie in Duitsland.

Kernfuncties en kenmerken van het platform

Virtualisatie / hypervisor

In een Rancher + KubeVirt-architectuur wordt virtualisatie niet geleverd door een traditionele type 1 hypervisor zoals ESXi, maar door

KubeVirt als extensie op Kubernetes. KubeVirt maakt het mogelijk om virtuele machines (VM's) als Kubernetes resources te draaien, waarbij QEMU/KVM wordt gebruikt op de onderliggende Linux hosts. Hierdoor kunnen VM's en containers naast elkaar bestaan en via één control plane worden beheerd.

KubeVirt benut hardware assisted virtualisatie (Intel VT x / AMD V) via KVM en biedt ondersteuning voor CPU pinning, NUMA awareness, hugepages en SR IOV voor netwerkintensieve workloads. Virtuele machines worden gedefinieerd via declaratieve YAML manifesten en vallen onder hetzelfde scheduling en lifecycle model als containers. Live migration van VM's is beschikbaar, mits gedeelde opslag en netwerkconfiguratie dit ondersteunen.

4

De schaalbaarheid van KubeVirt is direct gekoppeld aan de schaalbaarheid van Kubernetes. Clusters kunnen bestaan uit tientallen tot honderden nodes, afhankelijk van de gekozen Kubernetes distributie en infrastructuur. Rancher fungeert hierbij als centraal beheerplatform voor meerdere Kubernetes clusters, verspreid over datacenters of locaties.
Ondersteuning voor gast besturingssystemen is breder dan alleen Linux: KubeVirt ondersteunt ook Windows VM's, mits de juiste virtio drivers en configuraties worden toegepast. Certificering en formele support voor specifieke workloads (zoals SAP of Oracle) is echter beperkter en vaak afhankelijk van de gekozen Linux distributie, hardwareleverancier en supportcontracten.

Opslag en opslagintegratie

Opslag in een Rancher + KubeVirt omgeving wordt geleverd via Kubernetes storage abstraheringen zoals Persistent Volumes (PV's) en StorageClasses. KubeVirt maakt gebruik van dezelfde storage mechanismen als containers, waardoor integratie met bestaande CSI drivers centraal staat.

Ondersteunde opslagoplossingen omvatten onder andere Ceph (Rook), Longhorn, NetApp Trident, Dell CSI drivers en andere enterprise SAN/NAS oplossingen via iSCSI, Fibre Channel of NFS. Voor KubeVirt VM's worden disks gemapt op Persistent Volume Claims, waardoor VM data onafhankelijk wordt van individuele nodes.

4

Snapshots en clones van VM disks worden ondersteund, afhankelijk van de gebruikte CSI driver. Backup en disaster recovery worden meestal gerealiseerd met tooling zoals Velero, Kasten K10 of vendor specifieke oplossingen. Encryptie van data at rest is mogelijk via de onderliggende storage laag; KubeVirt zelf voegt hier geen eigen encryptiemechanisme aan toe.

In tegenstelling tot klassieke HCI oplossingen is er geen uniforme optimalisatie voor mixed storage tiers binnen één cluster. Performance en functionaliteit worden grotendeels bepaald door de gekozen storage backend en CSI implementatie.

(Software Defined) Netwerken

Netwerkfunctionaliteit in deze architectuur is gebaseerd op Kubernetes Open Virtual Networking (OVN) en Kubernetes Container Network Interfaces (CNI) in combinatie met KubeVirt netwerkextensies. OVN maakt een snelle ontwikkeling door en komt daarmee dichterbij de mogelijkheden van de marktleiders. Veelgebruikte CNI's zijn Calico, Cilium en Flannel, waarbij Cilium steeds vaker wordt ingezet vanwege eBPF gebaseerde observability en security.

4

KubeVirt ondersteunt verschillende netwerkmodellen voor VM's, waaronder bridge mode, masquerade en SR IOV voor near native performance. Load balancing en ingress voor applicaties worden doorgaans verzorgd via Kubernetes native ingress controllers of service meshes, terwijl VM gerichte load balancing vaak extern wordt opgelost.
Microsegmentatie en netwerkbeleid worden afgedwongen via Kubernetes Network Policies. In tegenstelling tot VMware NSX is er geen

volledig geïntegreerde L2–L7 SDN suite; functionaliteit wordt samengesteld uit meerdere open source componenten. Dit biedt flexibiliteit, maar verhoogt ook de architecturale complexiteit.

Bedrijfscontinuïteit
Hoge beschikbaarheid in een Rancher + KubeVirt omgeving wordt primair gerealiseerd via Kubernetes mechanismen. Wanneer een node faalt, worden VM pods opnieuw gestart op andere nodes, mits de VM definitie en opslag dit toelaten. Dit leidt doorgaans tot een korte onderbreking; automatische live failover zoals bij traditionele HA clusters is beperkt.

4

Live migratie van VM's is beschikbaar voor geplande onderhoudswerkzaamheden. Disaster recovery is geen standaardonderdeel van KubeVirt en vereist aanvullende tooling en architectuurkeuzes, zoals multi cluster setups en storage replicatie.

Beveiliging en compliance
Beveiliging en compliance worden grotendeels afgedekt door Kubernetes native functies. Authenticatie en autorisatie verlopen via Kubernetes RBAC, vaak geïntegreerd met externe identity providers zoals Active Directory, LDAP of OIDC.

4

VM's en containers vallen onder hetzelfde security model, inclusief namespaces, network policies en secrets management. Encryptie van data in transit wordt verzorgd via TLS binnen Kubernetes; encryptie at rest is afhankelijk van de storage laag. Audit logging en compliance rapportages vereisen aanvullende configuratie en vaak externe tooling.

Rancher biedt documentatie die gebruikers helpt om te voldoen aan verschillende beveiligingscertificeringen.

Beheer en automatisering

Ondersteuning en beheer van containers
Rancher is primair ontworpen als Kubernetes managementplatform en biedt uitgebreide ondersteuning voor containerplatformen. Het platform ondersteunt meerdere Kubernetes distributies (zoals RKE2, k3s, EKS, AKS en GKE) en biedt centraal clusterbeheer, policy management en role based access.

5

Rancher is primaier een container management platform; KubeVirt VM's worden aanvullend beheerd binnen hetzelfde ecosysteem. De focus blijft echter op containerapplicaties.

Lifecycle management
Lifecycle management van clusters en nodes wordt verzorgd door Rancher in combinatie met de gekozen Kubernetes distributie. Updates van Kubernetes versies, node besturingssystemen en componenten kunnen grotendeels geautomatiseerd worden, maar vereisen zorgvuldige planning.

3

Voor KubeVirt VM's bestaat geen centraal lifecycle mechanisme vergelijkbaar met vLCM. Updates van hypervisor componenten (QEMU/KVM) zijn onderdeel van het OS patchproces van de nodes.

Automatisering en orkestratie
Automatisering is een kernsterkte van dit platform. Declaratieve configuratie via YAML, GitOps modellen (bijvoorbeeld Argo CD of Flux) en integratie met CI/CD pijplijnen maken verregaande automatisering mogelijk. Integratie met tools zoals Terraform en Ansible is gangbaar,

5

maar minder gestandaardiseerd dan bij traditionele virtualisatieplatformen. Orkestratie richt zich vooral op applicatie en infrastructuurdefinities in plaats van individuele VM-operaties.

Observability en monitoring
Monitoring en observability zijn sterk afhankelijk van de gekozen stack. Prometheus en Grafana vormen vaak de basis, aangevuld met tools zoals Loki, Jaeger of commerciële oplossingen zoals Datadog en Dynatrace.

VM specifieke metrics zijn beschikbaar via KubeVirt exporters, maar bieden minder detail en volwassenheid dan traditionele hypervisor monitoring. Een uniform operations dashboard vereist integratie van meerdere componenten.

4

Integratie in bestaande beheersystemen
Rancher en Kubernetes hebben een groot open source ecosysteem en brede ondersteuning door leveranciers. Integratie met bestaande ITSM , monitoring en security tools is mogelijk, maar vergt maatwerk en architecturale keuzes.

De afwezigheid van één gecertificeerde marketplace zoals bij VMware betekent meer flexibiliteit, maar ook meer verantwoordelijkheid bij de afnemer.

4

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
De focus op containerapplicaties vraagt doorgaans een behoorlijke verandering in de organisatie, omdat de nadruk komt te liggen op het ontwikkelen van applicaties met behulp van containers. Virtuele machines kunnen nog wel, maar door de beperktere ondersteuning moet hier wel anders mee omgegaan worden dan met een volwaardig virtualisatieplatform. Ook dat heeft impact op hoe de organisatie moet opereren. Belangrijker nog is dat dit over het algemeen een transitie met zich meebrengt waarin applicaties aangepast moeten worden om in containers te kunnen werken. Adoptie van Rancher vergt daarom nieuwe vaardigheden van zowel ontwikkelaars als operations, maar biedt tegelijkertijd een versnelling in applicatieontwikkeling, schaalbaarheid en portabiliteit.

TB

Licentie en abonnement
Rancher (SUSE Rancher Prime) wordt aangeboden via abonnementen op basis van node aantallen. KubeVirt zelf is open source. Licentiekosten zijn doorgaans lager dan bij traditionele virtualisatieplatformen.

4

Overdraagbaarheid van licenties
Aangezien er voor Rancher Prime sprake is van een abonnement dat met name gericht is op ondersteuning van open source technologie, zijn er weinig beperkingen om naar een andere omgeving over te gaan. Voor de volledig open source variant van Rancher zijn er geen beperkingen.

5

Ondersteuningsmodel en ecosysteem
Ondersteuning is afhankelijk van de gekozen leverancier en de afbakening tussen Kubernetes, Rancher en onderliggende infrastructuur. Rancher Prime wordt ondersteund door Suse, wat een multinationale organisatie is met 2500 werknemers. Het ecosysteem rondom Linux en CNCF is groot, waardoor er veel expertise in de markt is.

4

Migratie en exit
Migratie van bestaande VM's naar KubeVirt vereist conversie en herontwerp. Er is beperkte tooling voor grootschalige VM migraties. Een overstap van Rancher Prime naar de volledige open source variant van Rancher is relatief eenvoudig te realiseren.

4

Door de brede ondersteuning van Rancher als open source platform is een gedwongen exit daaruit niet voor de hand liggend.

Innovatie
Innovatie verloopt snel, gedreven door de Kubernetes community. Nieuwe features verschijnen frequent, maar stabiliteit en lange termijn roadmap zijn minder voorspelbaar dan bij commerciële suites.

4

Omscholing en beschikbaarheid van talent
Kennis van Kubernetes is breed beschikbaar, maar expertise in KubeVirt is schaarser. Omscholing van traditionele virtualisatie specialisten is noodzakelijk en heeft een aanzienlijke leercurve. Suse en andere partijen bieden een breed scala aan trainingen en certificeringen aan.

4

Autonomie en continuïteit van de leverancier
Door het open source karakter is de autonomie hoog en vendor lock in beperkt. Continuïteit hangt echter af van de gekozen commerciële partij voor support en integratie.

5

Kosten (Total Cost of Ownership)
Hoewel Rancher Prime een initiële investeringsdrempel kent, kan het platform op langere termijn kosten besparen door hogere efficiëntie, automatisering en platformuniformiteit. Als er nog geen container kennis aanwezig is binnen de organisatie is dit wel een grote drempel. De impact op de organisatie en de mensen is dan hoog. De kosten van een eventuele exit zijn ook relatief laag omdat er allerlei alternatieven zijn die een groot deel van de functionaliteit bieden. Migratie is complex omdat het een compleet andere architectuur en denkwijze is.

2

Red Hat OpenShift

Red Hat OpenShift is een enterprise containerplatform gebaseerd op Kubernetes en gebouwd rondom de open source componenten van de Cloud Native Computing Foundation (CNCF). OpenShift biedt een volledig geïntegreerde Kubernetes-distributie met extra functies voor security, beheer en enterprise-ondersteuning.

In tegenstelling tot klassieke hypervisor-virtualisatie richt OpenShift zich primair op container applicaties. Het platform abstraheert infrastructuur via Kubernetes en maakt applicatie-implementatie onafhankelijk van de onderliggende hardware of cloud.
Red Hat OpenShift is gebouwd op open-source technologieën zoals Kubernetes, Red Hat Enterprise Linux (RHEL) en CRI-O (Container Runtime Interface voor Open Container Initiative), maar het wordt niet beschouwd als volledig open-source. Hoewel de broncode van de kerncomponenten open is, bevat de verpakte enterprise-distributie leverancier eigen, vooraf geconfigureerde plug-ins, ondersteunings- en beheertools die een betaald abonnement vereisen.

Red Hat is onderdeel van IBM en daarmee valt het onder de invloedsfeer van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

4

Virtualisatie/hypervisor
De onderliggende hypervisor is KVM, geïntegreerd in Red Hat Enterprise Linux CoreOS (RHCOS). Virtuele machines worden uitgevoerd in

pods via KubeVirt (zie Rancher Prime voor meer details over KubeVirt), waarbij OpenShift verantwoordelijk is voor scheduling, lifecycle-management en resource-isolatie. Live migratie, high availability en CPU- en geheugen-overcommitment worden ondersteund, binnen de grenzen van Kubernetes-architectuur en clusterconfiguratie.

KVM maakt gebruik van hardware assisted virtualisatie (Intel VT x, AMD V, IOMMU). KVM is breed ingezet binnen cloud omgevingen en staat bekend om zijn stabiliteit en volwassenheid. KVM is meer geschikt voor kleinschalige tot middelgrote omgevingen.
De schaalbaarheid is primair bepaald door de schaal van OpenShift clusters. OpenShift ondersteunt grootschalige clusters met meerdere availability zones, waarbij virtuele machines automatisch opnieuw worden ingepland bij node uitval. Ondersteuning voor gast besturingssystemen volgt de mogelijkheden van KVM en Red Hat Enterprise Linux, met gecertificeerde ondersteuning voor gangbare Linux distributies en Windows workloads, mits voldaan wordt aan de geldende configuratie en performance vereisten.

OpenShift Virtualization Engine is nadrukkelijk gepositioneerd als vervanger of aanvulling op traditionele virtualisatie in omgevingen waar Kubernetes het strategische platform vormt.

Opslag en opslagintegratie

OpenShift ondersteunt persistente opslag via de Kubernetes Container Storage Interface (CSI). Hierdoor kan opslag van verschillende leveranciers naadloos geïntegreerd worden. OpenShift Data Foundation (ODF) – gebaseerd op Red Hat Ceph Storage – biedt software-defined storage met block, file en object storage binnen het OpenShift cluster.

Daarnaast is integratie mogelijk met externe storageplatformen zoals NetApp, Dell, HPE, Pure Storage en cloud-native storage-diensten. Features zoals snapshots, replication en storage policies worden geleverd via CSI-drivers en dynamische provisioning.

3

Voor databeveiliging ondersteunt OpenShift encryptie van data-at-rest en data-in-transit, afhankelijk van de gebruikte storage back-end. Back-up en herstel zijn te realiseren via tools zoals Red Hat OpenShift API for Data Protection (OADP), gebaseerd op Velero, of via integratie met enterprise back-upoplossingen.

(Software Defined) Netwerken

Netwerkfunctionaliteit in deze architectuur is gebaseerd op Kubernetes Open Virtual Networking (OVN) en Kubernetes Container Network Interfaces (CNI) in combinatie met KubeVirt netwerkextensies. OVN maakt een snelle ontwikkeling door en komt daarmee dichterbij de mogelijkheden van de marktleiders. Veelgebruikte CNI's zijn Calico, Cilium en Flannel, waarbij Cilium steeds vaker wordt ingezet vanwege eBPF gebaseerde observability en security.

KubeVirt ondersteunt verschillende netwerkmodellen voor VM's, waaronder bridge mode, masquerade en SR IOV voor near native performance. Load balancing en ingress voor applicaties worden doorgaans verzorgd via Kubernetes native ingress controllers of service meshes, terwijl VM gerichte load balancing vaak extern wordt opgelost.

4

Microsegmentatie en netwerkbeleid worden afgedwongen via Kubernetes Network Policies. In tegenstelling tot VMware NSX is er geen volledig geïntegreerde L2–L7 SDN suite; functionaliteit wordt samengesteld uit meerdere open source componenten. Dit biedt flexibiliteit, maar verhoogt ook de architecturale complexiteit.

Bedrijfscontinuïteit□
OpenShift is ontworpen met hoge beschikbaarheid als uitgangspunt. Control plane- en worker-nodes worden redundant uitgerold, waardoor uitval van individuele nodes automatisch wordt gecompenseerd door Kubernetes self-healing.
Applicatiecontinuïteit wordt gerealiseerd via pod-restarts, rescheduling en replica-sets. Stateful workloads kunnen gebruikmaken van persistente volumes met replicatie en snapshots, afhankelijk van de storage-oplossing.

4

Voor disaster recovery ondersteunt OpenShift multi-cluster architecturen met behulp van Red Hat Advanced Cluster Management (ACM). Hiermee kunnen applicaties over meerdere clusters worden uitgerold, gesynchroniseerd en failover-scenario's geautomatiseerd.

Beveiliging en compliance
Security is een kernonderdeel van OpenShift. Het platform biedt standaard:
- Integratie met enterprise identity providers (LDAP, Active Directory, OAuth, OIDC)
- Role Based Access Control (RBAC) op Kubernetes-niveau
- Security Context Constraints (SCC) voor het afdwingen van minimale privileges
- Image scanning en signature verification

4

OpenShift maakt gebruik van SELinux, seccomp en container-isolatie om workloads te beschermen. Encryptie van secrets is standaard ingeschakeld. Audit logging en compliance-rapportages maken het mogelijk om te voldoen aan regelgeving zoals ISO, SOC en NIST.

Beheer en automatisering

Ondersteuning en beheer van containers
OpenShift is in de kern een containerplatform, waardoor de ondersteuning voor containerapplicaties uitstekend is en gecertificeerd als conform CNCF Kubernetes. Het platform biedt ontwikkelaars een self-service platform met CI/CD-integratie, image registries en ontwikkeltooling. Via OpenShift Pipelines (Tekton) en GitOps (Argo CD) kunnen applicaties geautomatiseerd worden gebouwd en uitgerold.

5

Ontwikkelaars werken met containers, terwijl beheerders volledige controle houden over policies, security en infrastructuur. Deze scheiding ondersteunt een DevSecOps-werkwijze.

Lifecycle management
Lifecycle management van clusters wordt ondersteund via Operator Lifecycle Manager (OLM). Operators beheren de installatie, upgrades en configuratie van platform- en applicatiecomponenten op een declaratieve manier.

4

OpenShift ondersteunt gecontroleerde upgrades met minimale downtime. Versiebeheer en compatibiliteit worden strikt bewaakt door Red Hat, inclusief langere supportcycli via EUS-releases.

Automatisering en orkestratie
Automatisering gebeurt primair via Kubernetes declaratieve configuratie (YAML) en APIs. OpenShift integreert met Ansible Automation Platform, Terraform en CI/CD-tools voor end-to-end orkestratie.

5

Red Hat Advanced Cluster Management maakt het mogelijk om meerdere OpenShift clusters centraal te beheren, inclusief policies, configuraties en applicatie-uitrol.

Observability en monitoring
OpenShift bevat standaard monitoring en logging op basis van Prometheus, Alertmanager en Grafana. Metrics zijn beschikbaar voor infrastructuur, clusters en applicaties.

4

Logging wordt geleverd via de OpenShift Logging Stack (Loki/Elasticsearch afhankelijk van configuratie). Integratie met externe observability-tools zoals Datadog, Dynatrace, Splunk en Grafana is breed ondersteund.

Integratie in bestaande beheersystemen
Red Hat heeft een uitgebreid ecosysteem van gecertificeerde partners via het Red Hat Partner Connect-programma. Veel enterprise tools ondersteunen OpenShift als deployment platform, waaronder CI/CD, security, observability en data platforms.

4

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie
De focus op containerapplicaties vraagt doorgaans een behoorlijke verandering in de organisatie, omdat de nadruk komt te liggen op het ontwikkelen van applicaties met behulp van containers. Virtuele machines kunnen nog wel, maar door de beperktere ondersteuning moet hier wel anders mee omgegaan worden dan met een volwaardig virtualisatieplatform. Ook dat heeft impact op hoe de organisatie moet opereren. Belangrijker nog is dat dit over het algemeen een transitie met zich meebrengt waarin applicaties aangepast moeten worden om in containers te kunnen werken. Adoptie van OpenShift vergt daarom nieuwe vaardigheden van zowel ontwikkelaars als operations, maar biedt tegelijkertijd een versnelling in applicatie-ontwikkeling, schaalbaarheid en portabiliteit.

TB

Licentie en abonnement
OpenShift wordt afgenomen via een abonnement per CPU-core (on-premises) of via cloud marketplace-modellen. Het abonnement omvat platformsoftware, updates en Red Hat enterprise support.

4

Overdraagbaarheid van licenties
Aangezien er sprake is van een abonnement dat met name gericht is op ondersteuning van open source technologie, zijn er weinig beperkingen om naar een andere omgeving over te gaan.

5

Ondersteuningsmodel en ecosysteem
Red Hat biedt enterprise support met duidelijke SLA's en langdurige productondersteuning. OpenShift heeft een groot en groeiend ecosysteem en wordt breed ondersteund door system integrators en cloud providers.

4

Migratie en exit
Migratie naar OpenShift vereist herarchitectuur of containerisatie van applicaties. Voor bestaande applicaties zijn er hulpmiddelen zoals OpenShift Virtualization (KubeVirt) om virtuele machines naast containers te draaien.

4

Exit-mogelijkheden zijn relatief gunstig doordat OpenShift gebaseerd is op open standaarden (Kubernetes, OCI-containers), waardoor applicaties makkelijker overdraagbaar zijn naar andere Kubernetes-platformen met ondersteuning van KubeVirt.

Innovatie
Red Hat investeert sterk in Kubernetes, hybrid cloud en edge-architecturen. Innovatie richt zich onder andere op AI/ML workloads, platform

5

engineering, GitOps en application services.

Omscholing en beschikbaarheid van talent

Er is een groeiend aanbod van OpenShift- en Kubernetes-specialisten. Red Hat biedt uitgebreide documentatie, trainingen en certificeringen (RHCSA, RHCE, OpenShift-specialisaties). Zoals gezegd bij Impact op de organisatie vereist OpenShift een significant verandering in hoe gewerkt wordt. Dit heeft initieel een hogere impact op omscholing, maar daarna is de opgedane expertise wel meer toekomstbestendig.

4

Autonomie en continuïteit van de leverancier

Red Hat is onderdeel van IBM, een kapitaalkrachtige partij met lange termijn focus op enterprise software. Doordat OpenShift grotendeels gebaseerd is op open source, is de afhankelijkheid van één leverancier beperkt in vergelijking met platformen waarvan het eigendom bij één partij ligt.

4

Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten Red Hat levert. De impact daarvan is beperkt doordat er geen connectiviteit nodig is om OpenShift te opereren. Verder kan met beperkte impact overgestapt worden naar OpenShift Origin, een volledig open source variant, of andere Kubernetes platformen\.

Kosten (Total Cost of Ownership)

Hoewel OpenShift een initiële investeringsdrempel kent, kan het platform op langere termijn kosten besparen door hogere efficiëntie, automatisering en platformuniformiteit. Als er nog geen container kennis aanwezig is binnen de organisatie is dit wel een grote drempel. De impact op de organisatie en de mensen is dan hoog. De kosten van een eventuele exit zijn ook relatief laag omdat er allerlei alternatieven zijn die een groot deel van de functionaliteit bieden. Migratie is complex omdat het een compleet andere architectuur en denkwijze is.

1

VMWare

VMware is de marktleider in de virtualisatiemarkt en biedt een zeer stabiel en uitgebreid platform. Het is echter negatief in het nieuws gekomen door de overname van Broadcom en de daaropvolgende aanpassingen in de licentiestructuur en kosten. VMware blijft echter een aantrekkelijk platform door de rijkheid aan functies en de grote hoeveelheid expertise in de markt. Broadcom is Amerikaans, hetgeen zorgen oplevert over de invloed van de Amerikaanse overheid.

Kernfuncties en kenmerken van het platform

Virtualisatie/hypervisor

Virtualisatie van hardware door een hypervisor wordt door VMware geleverd door vSphere, wat onderdeel uitmaakt van zowel VMware Cloud Foundation als VMware vSphere Foundation.
De hypervisor van VMware is marktleidend en biedt uitstekende stabiliteit, efficiency en schaalbaarheid. Daarnaast is de compatibiliteit met hardware en software zeer goed, met een duidelijk certificeringsprogramma.
ESXi is de hypervisor van VMware met bewezen betrouwbaarheid in enterprise-omgevingen. De hypervisor ondersteunt hardware-assisted virtualisatie (Intel VT-x, AMD-V) en MMU/I/O virtualisatie en biedt optimalisatie van CPU-, geheugen- en I/O-gebruik over verschillende hosts heen door vMotion, DRS, en vNUMA, wat efficiënt vebruik van resources mogelijk maakt.
vSphere heeft een hoge schaalbaarheid tot 64 hosts per cluster en 1024 virtuele machines per host. Daarnaast biedt vCenter multi-clusterbeheer en is het mogelijk om over meerdere datacenters te schalen.
vSphere heeft een brede ondersteuning voor gast operating systemen, waarbij VMware verschillende ondersteuningsniveaus onderscheidt. Verder ondersteunt vSphere software zoals Oracle RAC en SAP S/4 HANA (indien voldaan wordt aan de hardware voorwaarden).

5

Opslag en opslagintegratie

Opslag kan voor VMware vSphere op verschillende manieren geleverd worden. Ten eerste kan vSphere aansluiten op “traditionele” SAN (Storage Area Network) en NAS (Network Attached Storage). Daarnaast kan opslag op de ESXi hosts gebruikt worden om locale ops lag (alleen voor de betreffende host) en gedeelde opslag (gedeeld door meerdere hosts binnen een cluster) aan te bieden. Gedeelde opslag maakt hoge beschikbaarheid mogelijk. De derde optie is VMware vSAN, wat onderdeel uitmaakt van zowel VMware Cloud Foundation als VMware vSphere Foundation , waarmee een virtuele SAN gemaakt kan worden over meerdere clusters op basis van de mixed nodes (compute + opslag) of pure opslag nodes. Aangezien vSAN standaard meegeleverd wordt, is de onderstaande evaluatie daarop gebaseerd, tenzij anders aangegeven.

5

vSAN biedt betrouwbare opslag met verspreiding data over meerdere hosts op basis van configureerbare opslag policies. vSAN biedt daarbij ondersteuning voor mixed compute/opslag clusters en aparte storage clusters. Ook biedt vSphere integratie met externe SAN en NAS oplossingen van de meeste leveranciers (NetApp, Dell, HPE, Pure, etc.). Integratie met externe opslag kan daarbij met verschillende protocollen, waaronder NFS v3/v4.1, iSCSI, Fibre Channel.

Het veiligstellen van data kan via snapshots vanuit vSphere en Site Recovery Manager (SRM) voor noodherstel (disaster recovery). Beveiliging van data kan met vSphere Virtual Machine Encryption of vSAN encryption, waarbij beide gebruik kunnen maken van een externe Key Management Server voor extra beveiliging van encryptiesleutels.

TB

Optimalisatie van dataopslag gebeurt ten eerste standaard met block-level deduplicatie en compressie voor storage. Daarnaast maakt HCI Mesh het mogelijk om ongebruikte opslag in andere clusters te gebruiken. Indien verschillende typen opslag gebruikt worden is er geen optimalisatie van mixed-mode/asymmetrische opslag binnen een cluster en bepaalt de minst snelle opslag de snelheid van de gehele opslag.

(Software Defined) Netwerken

Voor netwerkfunctionaliteit biedt VMware twee opties:

3

- vSphere Networking is onderdeel van het vSphere virtualisatieproduct en is voor klanten van VMware vSphere Foundation de standaard. vSphere networking biedt verschillende mogelijkheden om virtuele machines toegankelijk te maken via het netwerk.

5

- VMware Cloud Foundation wordt geleverd met VMware NSX wat uitgebreide netwerkvirtualisatie levert, met veel verder gaande opties dan vSphere Networking. NSX biedt functionaliteit om zaken mogelijk te maken als het centraal en geautomatiseerd beheren van het hele netwerk, multi-tenancy en self-service voor een cloud-achtige ervaring, en microsegmentatie en encryptie voor de beveiliging van het netwerk.

Naast het bovenstaande kunnen klanten van zowel VMware Cloud Foundation als VMware vSphere Foundation gebruik maken van VMware Avi Load Balancer, wat load balancing ondersteunt voor zowel virtuele machines als containers en een geïntegreerde Web Application Firewall biedt voor bescherming van applicaties. Avi Load Balancer maakt het makkelijker om applicaties hoog beschikbaar te maken en te schalen.
Aangezien NSX niet beschikbaar is in VMware vSphere Foundation, is de evaluatie daarvan hieronder gescheiden.

vSphere Networking + Avi Load Balancer

Door jaren aan ontwikkeling is de stabiliteit van de netwerkfuncties in vSphere uitstekend. Daarbij is het zo dat een vSphere omgeving aangesloten moet worden op een bestaand netwerk. Het beheer van dat netwerk ligt buiten vSphere, vSphere beheert alleen de virtuele

netwerken binnen clusters.

Schaalbaarheid is beperkt tot de schaalbaarheid binnen een cluster en connecties met andere clusters via het aangesloten netwerk. De automatisering is daarmee ook beperkt tot automatisering binnen clusters.
Integratie met applicaties is deels te realiseren met Avi Load Balancer en de Web Application Firewall die daar deel van uitmaakt. Er is geen container integratie (VWware Tanzu Platform maakt geen onderdeel uit van VMware vSphere Foundation).

VMware NSX

VMware NSX is een van de marktleiders op het gebied van Software Defined Netwerken met hoge stabiliteit. Het ondersteunt uitgebreide hybride mogelijkheden via NSX Federation, VPN, BGP, EVPN; ondersteuning voor VMware Cloud & multi-site overlays. Volledig compatible met Cisco ACI, inclusief NSX+ACI co-existentie, L3Out en ACI Multisite ondersteuning.

NSX heeft een hoge mate van schaalbaarheid, ook over meerdere locaties via NSX Multisite of NSX Federation, waarbij ook gebruik gemaakt kan worden van automatisering via Aria Automation, PowerCLI en APIs. Integratie in 3rd party tools zoals Terraform en Ansible.
NSX-T biedt verschillende integratiemogelijkheden met L2–L7 networkfuncties (overlay, DFW, NAT, LB, DHCP/DNS, VRFs) en integratie met Kubernetes en OpenShift.

Bedrijfscontinuïteit□
VMware biedt functies voor hoge beschikbaarheid en noodherstel (disaster recovery) met vSphere High Availbility en vSphere Replication, wat onderdeel is van het vSphere product. High Availability zorgt ervoor dat een virtuele machine naar een andere ESXi host verplaatst wordt bij hardware falen en dit gebeurt automatisch. Als de virtuele machine daarbij uitgaat, is dataverlies beperkt tot onvoltooide diskoperaties. Bij falen van ESXi host worden de VMs automatisch op andere host opnieuw opgestart. Die starttijd van variëren (meestal 1-2 minuten). Met vSAN Stretched clusters is automatische site failover met witness mogelijk. Met vSphere Replication kunnen herstelpunten (recovery points) gemaakt worden waarnaar teruggegaan kan worden. Het Recovery Point Objective is instelbaar tussen 5 minuten en 24 uur en meerdere herstelpunten kunnen opgeslagen worden om te beschermen tegen data corruptie. Replicatie is eenvoudig te configureren.

5

Ook biedt VMware Site Recovery Manager (SRM) dat apart gelicenseerd dient te worden gebundeld met VWware Cyber Recovery onder de Live Recovery suite. SRM biedt additionele opties voor het beheren en orkestreren van noodherstelprocessen, testen van noodherstelplannen en replicatie van gehele opslag volumes (LUNs, VMFS of NFS) in plaats van replicatie op VM-niveau.

Beveiliging en compliance
Functies voor beveiliging en compliance zijn standaard onderdeel van VMware producten. vSphere ondersteunt standaard integratie met meerdere identiteitssystemen zoals Active Directory (AD), Active Directory Federation Services (ADFS) en LDAP. Met ADFS kunnen aanbieders van Multi-Factor Authentication als Duo of Ping gebruiky worden. Verder zorgt Role Based Access Control (RBAC) voor granulaire toekenning van rechten waarbij systeem- en User Defined rollen mogelijk zijn. Rollen kunnen gekoppeld worden aan locale accounts of accounts vanuit vCenter SSO.

5

Encryptie met integratie met een Key Management Server zorgt verder voor veilige opslag van data.
Audit logs en monitoring functies bieden mogelijkheden om het platform veilig en conform configuratie te houden, zodat ook compliance aangetoond kan worden. Monitoring is mogelijk op CPU, geheugen, disk en netwerk, en biedt de mogelijkheid voor grafische weergave, notificaties en alarmfuncties. Met VMware Aria Operations for Logs kan ingesteld worden welke log events bewaard moeten blijven.

VMware NSX biedt ook mogelijkheden om het netwerkverkeer te versleutelen, ongeacht het applicatieprotocol. Wanneer NSX niet gebruikt wordt, is de versleuteling van netwerkverkeer de verantwoordelijkheid van applicaties of van de netwerk stack die toegepast wordt.

Beheer en automatisering

Ondersteuning en beheer van containers

VMware biedt Kubernetes via VMware Tanzu Platform (Tanzu), wat onderdeel is van VMware Cloud Foundation. Tanzu integreert met het verdere VMware platform, zodat rekenkracht, opslag en netwerk integraal beheerd kan worden. Tanzu is CNCF gecertificeerd en een verfijnd product met een gebruiksvriendelijke manier om Kubernetes te gebruiken en beheren.

4

Tanzu Kubernetes Grid biedt schaalbaarheid en redundatie op basis van Availability Zone concept met verdeling over meerdere vSphere clusters. Tanzu biedt geen diepe infrastructuurintegratie om alle beheer onder een dak te brengen, maar virtuele machines kunnen wel in Tanzu beheerd worden naast containers binnen een vSphere namespace.

Lifecycle management

Lifecycle management functionaliteit wordt geboden door vSphere Lifecycle Management (vLCM), hetgeen beschikbaar is voor zowel VMware Cloud Foundation en VMware vSphere Foundation.
vLCM maakt gebruik van declaratieve Desired State configuratie, waarmee aangegeven wordt welke software, firmware en drivers op hosts geïnstalleerd moeten zijn. Daarbij kan het zowel VMware als de updates van de infrastructuurleverancier uitrollen. Reduced Downtime Upgrade (RDU) en Distributed Resource Scheduling (DRS) kunnen gebruikt worden om rolling updates te doen en patching te verzorgen zodat virtuele machines zeer beperkte downtime hebben.

5

Organisaties die configuratie management doen met tools als Ansible, Chef Puppet of Terraform, kunnen daar ook gebruik van maken om lifecycle management te ondersteunen binnen virtuele machines en voor de infrastructuur.

Noot: VMware Cloud Foundation Operations biedt lifecycle management voor private cloud, maar valt buiten de scope van dit rapport.

Automatisering en orkestratie

VMware maakt een hoge mate van automatisering mogelijk via Power CLI en VWware Aria Suite (voorheen vRealize), met versiebeheer en terugrol-mogelijkheden, waardoor het geschikt is voor grote omgevingen met veel clusters. Ook is er brede integratie met 3rd party tools zoals Ansible, Chef, Puppet en Terraform.

5

De drag-and-drop Workflow Designer en een uitgebreide bibliotheek met standaard workflows maken het eenvoudig om taken te automatiseren.

Observability en monitoring

VMware producten zijn over het algemeen vooral gericht op integratie met eigen tooling, maar bieden daardoor wel een hoge mate van gebruiksgemak om alle onderdelen van de VMware omgeving te monitoren. De observability functies werken daardoor het beste als ze gebruikt worden in een volledige VMware omgeving en bieden daarvoor uitgebreide meetpunten voor CPU, geheugen, disk en netwerkoperaties. VMware Cloud Foundation (VCF) Operations is een gehele operations suite voor het beheren van VMware-gebaseerde private cloud omgeving. VCF Operations biedt een Splunk Add-on om geavanceerde analyse te doen met Splunk.

5

Organisaties die VMware vSphere Foundation gebruiken, zijn aangewezen op de monitoring van vSphere en 3rd party tools zoals Datadog, Dynatrace, Grafana, Splunk en Unryo.

Integratie in bestaande beheersystemen

VMware heeft via hun Technology Alliance Partner (TAP) programma en de VMware Markerplace een groot aanbod aan tools dat integreert met de VMware suite. De mate van integratie van deze tools is groot, omdat er gewerkt wordt met een certificeringsprogramma. VMware representeert al jaren een grote afzetmarkt, waardoor ook andere leveranciers tooling hebben ontwikkeld die integreert VMware functionaliteit. Voorbeelden hiervan zijn:

5

- New Relic integraties met vSphere en Tanzu, waardoor het samen monitoring van applicaties een totaalbeeld kan geven van hoe applicaties en infrastructuur opereren.
- Rubrik integratie voor backup en noodherstel, inclusief referentiearchitecturen voor VCF.
- VMware licentieoptimalisering met Flexera.

Bedrijfsvoering, operationele factoren en kosten

Impact op de organisatie

Aangezien VMware de marktleider is voor virtualisatieplatformen, is de impact op de organisatie waarschijnlijk beperkt, tenzij de organisatie geen virtualisatieplatform had en/of er meer prioriteit gegeven wordt aan containerapplicaties.

TB

Licentie en abonnement

VWware is overgestapt naar een abonnementsmodel, waarbij het gebruiksrecht voor een bepaalde tijd wordt afgenomen. VMware bundelt daarbij verschillende producten onder een abonnement, waardoor het inefficiënt is om alleen bepaalde componenten te gebruiken. Dat maakt het abonnement op zich relatief transparant en simpel, maar brengt wel hoge kosten met zich mee. In een langdurig contract worden ook standaard jaarlijkse prijsverhogingen opgenomen.

3

Overdraagbaarheid van licenties

VMware-licentieportabiliteit stelt klanten in staat hun VMware Cloud Foundation (VCF)-licenties te nemen en deze te laten draaien in gevalideerde omgevingen, waaronder on-premises, edge-implementaties en geautoriseerde partnerclouds, zonder opnieuw te hoeven kopen of opnieuw te licenseren.

4

Ondersteuningsmodel en ecosysteem

VMware biedt als onderdeel van hun licenties ondersteuning voor de VMware Cloud Foundation en biedt daarbij voor grotere klanten ook Technical Account Management. Uit praktijkervaringen blijkt echter dat niet alle klanten goede ondersteuning ervaren. Broadcom stelt vrij strenge implementatie-eisen om in aanmerking te komen voor ondersteuning, bijvoorbeeld vereisten dat bepaalde functies geïmplementeerd zijn.

Een nieuwe versie van VMware Cloud Foundation kan iedere 2 jaar verwacht worden, met updates iedere 9 maanden. Er is geen vast schema voor het uitbrengen van patches.

4

Omdat VMware de marktleider is, is het ecosysteem rondom VMware groot en is er veel kennis in de markt bij system integrators en managed service providers.

Migratie en exit

VMware biedt ten eerste tooling om te migreren tussen VMware omgevingen, eventueel met verschillende versies, met vMotion, Hybrid Cloud Extension (HCX) en Site Recovery Manager. Verder biedt VMware de mogelijkheid om fysieke servers naar VMware te migreren met P2V. Deze tooling is allemaal zeer volwassen.

Tooling om naar andere virtualisatieplatformen te migreren worden met name geleverd door andere partijen, hetzij als losse tooling (bijvoorbeeld Veeam) of als onderdeel van tooling van een concurrent om naar hen toe migreren, waaronder Microsoft (Hyper-V, Azure Local en Azure Cloud), Nutanix en Red Hat.

4

Naarmate meer van de VMware suite gebruikt wordt, wordt het lastiger om een exit te maken, omdat de integratie van de verschillende onderdelen hoog is. Dit geldt vooral als gebruik gemaakt wordt van netwerkintegratie met NSX. De complexiteit van migratie zit niet in de migratie van individuele virtuele machines of zelfs groepen daarvan, maar het overzetten van de gehele omgeving.

Innovatie

VMware blijft fors investeren in nieuwe versies met nieuwe features. Een nieuwe versie wordt iedere 2 jaar verwacht, met tussentijdse updates iedere 9 maanden. Hierbij wordt onder andere geinvesteerd in de toepassing van Data Processing Units (DPUs), het kunnen toepassen van AI, Aria als management suite voor private cloud omgevingen, en Kubernetes via Tanzu. Daarmee heeft VMware een roadmap met veel nieuwe mogelijkheden die ontwikkeld worden.

4

Omscholing en beschikbaarheid van talent

VMware heeft een uitgebreid trainings- en certificeringsprogramma op basis van goede documentatie voor zelfstudie, een digitale leeromgeving en training van een instructeur (door VMware zelf of een 3e partij). Doordat VMware de marktleider is, is er aan beschikbare expertise in de markt geen gebrek, al hebben de stijgende licentiekosten wel tot gevolg dat meer mensen naar alternatieven kijken.

5

Autonomie en continuïteit van de leverancier

Om VMware Cloud Foundation te kunnen blijven gebruiken, moet periodiek een validatie uitgevoerd worden van de licenties. Dit dient iedere 180 dagen te gebeuren en hiervoor zijn twee verschillende mogelijkheden, waarbij het mogelijk is om van de ene manier over te schakelen naar de andere:

- Connected: Connected mode is het gemakkelijkst voor de klant, want binnen elke 180 dagen moet een klant op één knop klikken om de licentie-gebruiksinformatie in te sturen.
- Disconnected: Klanten met de disconnected-modus moeten hun licentiegebruiksbestand handmatig uploaden naar het Broadcom-supportportaal vcf.broadcom.com en vervolgens het licentiebestand binnen 180 dagen downloaden naar VCF Operations om aan de licenties te voldoen.

Effectief betekent het bovenstaande dat wanneer VMware om wat voor reden dan ook licenties niet gevalideerd kunnen worden, dat dit gevolgen heeft voor de draaiende omgeving. Daarmee heeft de licentievalidatie invloed op de autonomie van de afnemer.
VMware is onderdeel van Broadcom, wat een kapitaalkrachtige partij is met een marktwaarde van ca. 1,5 biljoen USD en winst van ca. 40 miljard USD per jaar (January 2026). De continuiteit van VMware is daarmee hoog en de kans op overname door een derde partij klein.
Als Amerikaans bedrijf, heeft de Amerikaanse overheid wettelijke mogelijkheden om te beperken aan welke klanten VMware levert.

3

Kosten (Total Cost of Ownership)

Hoewel de licentiekosten van VMware door de veranderingen in licentiestructuur aanzienlijk toegenomen zijn, zijn er verschillende factoren die de totale kosten voor het platform omlaag brengen, zoals brede hardware ondersteuning, ondersteuning door de leverancier, en hoge beschikbaarheid van expertise.

3

Appendix D - Andere alternatieven

In de gesprekken die gevoerd zijn voor dit rapport zijn ook andere alternatieven besproken. Om verschillende redenen zijn deze niet opgenomen in de vergelijking. Hieronder worden deze oplossingen kort besproken met de redenen waarom ze niet opgenomen zijn.

AWS Outposts

AWS Outposts is een on-premises infrastructuur voor clouddiensten van AWS. Het biedt daarmee veel van de functionaliteiten die van toepassing zijn voor een virtualisatieplatform. AWS Outposts vereist echter een vrijwel permanente verbinding met een AWS regio. Deze afhankelijkheid maakt deze oplossing even kwetsbaar qua autonomie als het directe gebruik van de AWS cloud zoals besproken onder Infrastructure-as-a-Service Clouddiensten.

Citrix

Citrix Hypervisor (tegenwoordig bekend onder de naam XenServer) heeft een sterke focus op het bieden van een hypervisor voor Virtual Desktop Infrastructure (VDI) voor Citrix en doorontwikkeling is beperkt. Daarmee is het niet gericht op de primaire scope van dit onderzoek.

Google Distributed Cloud (Air-gapped)

Google Distributed Cloud (Air-gapped) is een private cloud oplossing die de functionaliteit van de Google Cloud in het eigen datacenter plaatst. Hierbij wordt hardware en software geïntegreerd geleverd en geopereerd door een derde partij. Dit is dermate anders dat het opereren van een virtualisatieplatform, dat een vergelijking daarmee per definitie ongelijk is.

HPE Private Cloud Enterprise

HPE Private Cloud Enterprise is, zoals de naam ook al suggereert, een private cloud oplossing die cloud-functionaliteit in het eigen datacenter plaatst. Hierbij wordt hardware en software geïntegreerd geleverd en geopereerd door een derde partij. Dit is dermate anders dat het opereren van een virtualisatieplatform, dat een vergelijking daarmee per definitie ongelijk is.

Infrastructure-as-a-Service Clouddiensten

Cloud providers zoals AWS, Google, Microsoft, Oracle, OVH, Scaleway en StackIT bieden voor het uitvoeren van virtuele machines en containers vergelijkbare functionaliteit t.o.v. de verschillende virtualiseringsplatformen, inclusief de aanpalende functionaliteiten voor o.a. automatisering, beheer, beveiliging, monitoring, observability en orchestratie. Aangezien veel softwareleveranciers een “cloud first” beleid hanteren, bieden met name de grote cloud providers goede integratie met allerlei 3rd party functionaliteiten. Functioneel gezien is daarmee vrijwel alles te realiseren wat organisaties in hun eigen datacenter uitvoeren op basis van een virtualisatieplatform en bieden deze cloud providers ook allerlei functionaliteit die het mogelijk maken applicaties te moderniseren en bijvoorbeeld gebruik te maken van containers en Platform-as-a-Service diensten die meer functies bieden.

De geopolitieke situatie maakt het echter niet voor de hand liggend om operationele controle over te laten aan een cloud provider, aangezien de voornaamste kandidaten gevestigd zijn in de Verenigde Staten. Verder vergt dit een complete technische herziening van de (virtuele) infrastructuur, omdat de architectuur en alle APIs anders zijn.

Oracle OVM

Oracle OVM is gemarkeerd als einde van de levensduur en wordt niet meer verder ondersteund door Oracle. Oracle Linux Virtualization Manager beschreven in Appendix C – Virtualisatieplatformen is de opvolger van Oracle OVM.

In de gesprekken die gevoerd zijn voor dit rapport zijn ook andere alternatieven besproken. Om verschillende redenen zijn deze niet opgenomen in de vergelijking. Hieronder worden deze oplossingen kort besproken met de redenen waarom ze niet opgenomen zijn.

VMware in Cloud

Hoewel bestaande klanten van VMware diensten op cloud providers als AWS en Microsoft nog enige tijd gebruik kunnen maken van deze dienst zonder een licentie van Broadcom, dienen nieuwe klanten die gebruik willen maken van VMware diensten bij cloud providers daarvoor zelf een VMware Cloud Foundation licentie te verzorgen. Migratie naar een van deze clouddiensten heeft derhalve geen voordelen meer om licentiekosten te beperken. VMware in Cloud is eventueel een optie in gevallen waar tijdelijk geen hardware beschikbaar is om (een deel van de) applicaties uit te voeren.